UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
------------------------------x

UNITED STATES OF AMERICA,

v. 17 Cr. 548 (JMF)

JOSHUA ADAM SCHULTE,

Defendant.

Trial (Redacted)

------------------------------x

New York, N.Y.
June 27, 2022
9:00 a.m.

Before:

HON. JESSE M. FURMAN,

District Judge
-and a Jury-

APPEARANCES

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
BY: DAVID W. DENTON JR.
MICHAEL D. LOCKARD
Assistant United States Attorneys

JOSHUA A. SCHULTE, Defendant *Pro Se*

SABRINA P. SHROFF
DEBORAH A. COLSON
Standby Attorneys for Defendant

Also Present: Charlotte Cooper, Paralegal Specialist

(Trial resumed; Jury not present)

THE COURT: Good morning. I hope everyone had a good weekend. A couple jury-related issues before we proceed.

I don't know if you have already heard this, we had one unfortunate development over the weekend. Juror No. 14 tested positive for COVID on Saturday. I emailed the rest of the jury yesterday to let them know and to ask them to show up early today to get molecular rapid tests at the DE's office. Last I heard, 13 of 15 had showed up so we are just waiting on the last two. So far all tests are negative, although I think only five of the tests have come back. So we will keep our fingers crossed that there is no spread. My inclination would be to start -- as long as the other two show up and get tested, my inclination would be to start on the theory that if I am notified of any positive tests we can always break and take appropriate steps at that time. But it is an unfortunate situation I have. I obviously excused juror No. 14. If she is the only one who tests positive then I think we will have gotten off lucky since she was the juror with travel plans in a couple weeks anyway and likely wouldn't have made it to the end of this case but we will see what happens.

Second thing, Ms. Shroff. I don't know if you want to put on the record, my understanding you is you were in an elevator and inadvertently had an interaction although it sounded relatively innocuous from the description that I got but do you want to just make a record about that?

MS. SHROFF: Sure. Good morning, your Honor.

I was transferring the box of documents for this morning from the SCIF to 15A. I changed elevators on the eighth floor bank. The gentleman from Fed Cap who knows me was kind enough to hold the door open so I entered the elevator, and since I had the box I just leaned the box on the side of the elevator so my back was to the -- my back was not in the normal position of being to the back of the elevator. I didn't see anybody in there and then a voice asked me which floor I wanted to go to and I just replied I have it, it's 15A, thank you; or 15A, but I got it. Something like that. I can't remember the sequence. And then, when the elevator next opened it was on the 11th floor and a man exited, and when he exited I realized that it was juror no. 7. I didn't say anything more. He didn't see anything other than my back as far as I can tell but I don't know.

THE COURT: That sounds relatively innocuous to me. If the government has any concerns, speak now or hold your peace but I think we should just leave it as is.

All right. Anything that you guys want to discuss? The last two jurors have now shown up and they are being taken down for testing. Again, my intention is to begin once they have actually tested on the theory that we can break if there is need to but anything that you need to raise, either follow up on issues that were discussed on Friday or otherwise?

MR. LOCKARD: Not from the government, your Honor.

THE COURT: Mr. Schulte?

MR. SCHULTE: So the entire transcript of Mr. Leedom I think has been designated classified and so we were trying to get a feel for when we could get redacted copy of the transcripts, when those would be available so I can take it with me. And then, I just needed a couple minutes to review some of these files or some of these evidence things that were just presented to us that I hadn't had a chance to look at yet.

THE COURT: OK. What are those things?

MR. SCHULTE: I am trying to figure that out.

MR. LOCKARD: Your Honor, those are hard drives that have already been admitted into evidence pursuant to stipulation. We expect Mr. Berger will identify them and describe them and so we provided the physical exhibits to Mr. Schulte this morning so he could inspect them before that happened.

THE COURT: Gotcha. Well, if they're in evidence they're in evidence. And, I think you will have a couple minutes before we start in any event.

Government, I could ask the court reporter but do you know timing on the redaction of the transcript?

MR. DENTON: So, your Honor, we got the classified copy of the transcript this morning. I think the relevant folks are taking a look at it to see whether the redaction proposal is necessary at all. Hopefully we can report back either at the lunch break or certainly at the end of the day whether we anticipate making such a proposal at all and trying to move this as expeditiously as we can.

THE COURT: I'm confused. Didn't you raise one issue and we took care of that on Friday?

MR. DENTON: Yes, your Honor; that dealt with the previous testimony. I think this dealt with a discrete issue that everyone made some notes about on Friday during Mr. Leedom's cross-examination and so I think just without the benefit of the transcript it was hard to tell whether we were over the line or not. And so now that we have it, the relevant folks are looking at it as quickly as we can.

THE COURT: So you think you can let me know during the lunch break or at the end of the lunch?

MR. DENTON: I certainly hope so. If not, we will let the Court know where things stand and why.

THE COURT: OK. So get the word out that I would like to know at the end of the lunch break and, if not, I expect to be told when we will know and hopefully by the end of the day at the absolute latest.

Anything else? Otherwise, Mr. Schulte can examine the hard drive while we are waiting for the jury to come up but we should get Mr. Berger in here if there is nothing else to discuss.

Let's get Mr. Berger and I will keep you posted about the jury.

(pause)

THE COURT: Just a heads up that the jury is heading up now.

THE DEPUTY CLERK: Jury entering.

(Continued on next page)

(Jury present)

THE COURT: Good morning, ladies and gentlemen. Welcome back. I hope you all had pleasant weekends and enjoyed the nice summer weather.

Well, I know you all know the news over the weekend that one of you, namely juror No. 14, tested positive for COVID on Saturday. Thankfully she notified us and we were able to get in touch with you and ask you to all come and get tested this morning. So she is not here but I will thank her later for her conscientiousness for doing that. A reminder that we are not out of the woods and there is a good reason that we are taking all of the precautions that we are taking. Hopefully, in light of those precautions, everyone here will be fine and test negative. I know some of you were awaiting results of the tests and I will certainly alert you when I hear to let you know if anyone tests positive, we will take a break and obviously take necessary steps at that time but I thought we should get started in the meantime.

A few things. First of all, jurors no. 15 and 16, you are welcome to stay where you are if you have settled into those seats and you like them but you are also welcome to slide over if you prefer. I leave that to you.

Second, I'm going to ask you, for the next few days -- my understanding from the epidemiologist who advises the Court is if everyone tests negative this morning is that the odds of anyone testing positive as a result of any exposure to juror No. 14 are quite low given the number of days that have passed. Again, hopefully everyone has complied with the precautions. I will note, in case you all didn't figure it out, you are all fully vaccinated, most of you are boosted, so hopefully everyone will stay safe and healthy. I am, nevertheless, going to ask you, if you can, show up a couple minutes early for the next few days to the District Executive's office on the eighth floor where you went this morning to just get tested each morning. I think the next few mornings it will just be a regular rapid test. You are welcome to take one at home if you prefer to do it that way, but we will make testing available to you to make sure if anyone does test positive a few days out that we minimize the consequences of that.

Most importantly, I hope everybody obviously stays safe and healthy. I think juror No. 14 is generally doing fine so I will check in on her later and keep you posted but she has been excused from jury service given that she wouldn't be able to come for some number of days.

So with all of that, we will pick up where we left off on Friday with the direct testimony of Mr. Berger.

Mr. Berger, you can remove your mask at this time. I remind you that you remain under oath.

With that, we can proceed. Mr. Lockard?

MICHAEL BERGER, resumed.

DIRECT EXAMINATION

BY MR. LOCKARD:

Q. Good morning, Mr. Berger.

A. Good morning.

Q. So on Friday you reviewed some evidence that you had analyzed relating to the defendant's home computers and user activity. Do you remember that?

A. Yes, I do.

Q. Specifically activity relating to the Tails operating system and data destruction utilities?

A. Yes.

Q. So we will return to the defendant's home computer equipment in a little bit but first let's turn to another aspect of your analysis. Did you also review data obtained from the CIA's DevLAN system?

A. Yes, I did.

Q. And, broadly, what topics did that review cover?

A. The topics covered included permission changes made by defendant, as well as the data itself that was exposed by WikiLeaks.

MR. LOCKARD: Ms. Cooper, if we could please turn to page 5 of Government Exhibit 1704?

Q. Mr. Berger, is this some of the data that you pulled from the DevLAN system?

A. Yes, it is.

Q. Can you just give us a general description of what is reflected in here?

A. So this is a reconstruction from a Stash database backup file, specifically the Stash backup made on April 16th, 2016. What we are looking at is the results of a, what is called a SQL query. SQL is Structured Query Language, it is a programming language used to interact with the database. What we are looking at on the screen are the results of a particular query that was designed to show the activity pertaining to permission changes; anything relating to the user Schuljo from the dates April 4th through April 14th, of 2016.

Q. So focusing in on the events of April 14th -- if we can please move to the next slide, page 7, actually? Are these permission changes on April 14th?

A. Yes, they are.

MR. LOCKARD: Let's turn to page 8.

Q. Can you just describe what permission changes happened here?

A. So on April 14th of 2016 at 4:05 p.m. local time there was a permission request event which the specific event was to -- the specific event dealt with the project admin status for the user Schuljo. Specifically, the user account Schuljo requested admin privileges for the user account Schuljo for the project OSB Libraries. The request was made and the request was granted.

Q. Mr. Berger, do you recall during the testimony of Mr. Leedom that Mr. Leedom had reviewed a log file entry related to this request?

A. Yes.

Q. And do you recall the format of the timestamp on that log file entry?

A. Yes.

Q. Generally, what was the timestamp format on that log file entry?

A. The timestamp format was what is referred to as Epic Time.

Q. And did you convert that into Eastern Daylight Time?

A. Yes, I did.

Q. And what time did that convert into?

A. 4:05 p.m. on April 14th, 2016.

Q. The same time reflected in the data that you pulled?

A. Correct.

MR. LOCKARD: If we can please turn to page 9?

Q. Mr. Berger, can you describe where you obtained this data and what it reflects?

A. So this data, again, was provided by the CIA. What we are looking at are two different query results. One was made from the Crowd backup of April 15th, 2016. The next was from the Crowd backup of April 17th, 2016.

Q. And those are both queries with respect to the Schuljo user?

A. Correct. So these queries were designed to show any groups relating to the user account Schuljo; essentially, what groups was the user account Schuljo a member of on each of those dates.

Q. And after April 16th, was Mr. Schulte a member of the Atlassian administrators group?

A. After the 16th he was the not.

Q. Was he a member of the OSB group?

A. He was not.

MR. LOCKARD: If we can look at page 10?

Q. Here are some additional results relating to administrator privileges. Can you just describe what is shown in this slide?

A. So, again, using the Crowd backups from April 15th and April 17th, the queries ran reflect what users are members of the groups that have the word "administrator" in them. So on April 15th we are looking at any user that are members of any administrator group. On April 17th we are looking at the same query with much fewer results.

Q. And again, after April 16th, who were the members of the administrator groups in the Crowd database?

A. So on April 17th there are only two accounts listed as members of administrator groups.

Q. Now, Mr. Berger, did you review the defendant's online activities after April 14th as well?

A. Yes.

MR. LOCKARD: Ms. Cooper, can we please turn to page 51?

Q. Mr. Berger, what is reflected here?

A. So what we are looking at here are the results under the defendant's Google searches, specifically a search for Confluence admin view restricted pages, and then websites that the defendant visited after retrieving those search results.

Q. And what search did the defendant run on April 15th at 2:43 p.m.?

A. The search query was for Confluence admin view restricted pages.

Q. If we could look at page 52, please? What date are these searches from?

A. These are from April 18th, 2016.

Q. What did the defendant search for on April 18th of 2016 at 2:09 p.m.?

A. At 2:09 p.m. he searched for Linux copy file, as well as Linux copy file over network.

THE COURT: Can we just break for a second?

I heard a phone go off. Just a reminder, I think it is better to keep your phones in the jury room but if you have them here, take a moment to shut them off, please, so that you are not distracted in any way, shape, or form.

Good to go? Thank you.

You may proceed.

BY MR. LOCKARD:

Q. Thank you, your Honor.

Turning to 2:12 p.m. on April 18th, what did the defendant search for?

A. He searched for Linux copy large files hash.

Q. And just a couple lines above that one minute earlier, what did he search for?

A. He searched for copying multiple files, Linux large files.

Q. What is the relationship between hashing, which you described on Friday, and large file copying over a network?

A. So hashing is a way that you can fingerprint a set of data. If you have the same input data into the same hashing algorithm you will always get the same result. What is commonly used in copying data, is if you copy the data and you hash the source data and you hash the data that you have now copied, and they're identical, that indicates that there were no errors in the copying of that data and you have an identical duplicate copy of your original data.

MR. LOCKARD: Ms. Cooper, if we could please look at page 53?

Q. And there are a number of entries here. Can you generally summarize what types of searches were being run on April 19th of 2016?

A. So initially at 11:36 a.m. there was a search for fast hashing algorithm, and then there were additional hash algorithms searched for and pages visited reflecting different hashing functions. There is also a search down at 11:36 p.m., a search for fast hashing algorithm.

Q. Mr. Berger, based on your experience as a forensic analyst, what significance does fast hashing have in investigations that you conduct?

A. So if you are trying to hash a very large source of data it can take a considerable amount of time. There is a relationship between the larger the data size that you are trying to hash, the longer it takes. In this case it seems that the defendant was looking for a fast hashing algorithm as there are many different hashing algorithms out there and some are faster than others.

Q. And then with respect to the searches conducted on April 18th relating to the transfer of files over Linux, what operating system did the Atlassian products on DevLAN run?

A. They ran on Linux.

Q. So Mr. Berger, I think you said you also reviewed the data that was released by WikiLeaks?

A. Correct.

MR. LOCKARD: Ms. Cooper, if we can turn to page 14?

Q. What was the type of analysis that you conducted sort of broadly, and then we will focus in on some of particular steps that you took.

A. So I was asked to conduct a timing analysis specifically to look at the data that was on WikiLeaks, what was the date of that data, so what point was that data saved onto the DevLAN system.

Q. And how did you go about performing that analysis?

A. So in order to do that, utilize the concept of version control that both Stash and Confluence had some mechanism of within them I looked for data points, specifically data that was saved in one of those products that was also present on WikiLeaks, as well as data that was saved in those systems that was not present on WikiLeaks. Then we looked to see if we could find points that were as close together as possible to have a narrow range of when, exactly, the data was from.

Q. And when you were looking at data that was saved on the DevLAN system, where were you looking?

A. I was looking in both Stash and Confluence backups.

Q. And why did you focus on the backups in particular?

A. Because that's the data that we were provided by the CIA and we had the kind of idea of where to look and it was also the most helpful in terms of being able to access the raw data that was saved in the database.

Q. And were you also present during Mr. Leedom's testimony about his analysis that the source of the data did come from a backup file?

A. Yes.

Q. So let's start with Stash. Can you remind us again just the basic purpose or function of Stash?

A. So Stash was a source code repository. As developers would write code, they would save changes into a particular project repository within Stash.

Q. And how did you conduct a timing analysis on the Stash data?

A. So I looked for files that were included in the WikiLeaks release, specifically source code files that I could also identify within the Stash system.

Q. And how did you identify where identical files appeared?

A. So I was -- I used a hash algorithm to look for identical files.

Q. Let's look at what is shown here on page 14, focusing on the file identified as Marble.horig. Is that a file that was in the Vault 7 release?

A. Yes.

Q. And did you compute a hash value for it?

A. I did.

Q. Is that the long string of letters and numbers that is reflected on the screen?

A. It is.

Q. Did you find Marble.horig in the stash backups?

A. I did.

MR. LOCKARD: If we can turn to the next page, please?

Q. Can you show us what is shown in this table?

A. So this is a listing of commits for the file Marble.horig. A commit is every time that the file was saved into the system. We can see here by this table that there are several entries going from February 267 through March 7th where that particular file was saved and the value or the hash value of that particular commit is calculated and shown on the right. The entries on February 26, 2016 at 9:36 a.m., as well as March 1, 2016 at 11:09 a.m., indicate a hash mash for the file that was found on WikiLeaks.

Q. Mr. Berger, what are the reasons why there might be a file with the same hash value at two different commit times in the stash log?

A. So it is possible that whoever was working on this particular file made a change on February 26 at 9:37 a.m. and decided they didn't like that change and maybe wanted to revert back to the previous version. They would have reverted back to the February 26 9:36 a.m. version and then re-committed that version on March 1, 2016, at 11:09 a.m.

MR. LOCKARD: If we can turn to page 16, please?

Q. And does this show that same analysis in timeline format?

A. Yes.

Q. And so what did this indicate about the date range of data from Stash that was released by WikiLeaks?

A. This indicated that the data that WikiLeaks disclosed had to come from a point in time after February 26, 2016, at

9:36 a.m.

Q. And did it indicate anything about the latest date that the data could have come from?

A. Yes.

Q. What did that indicate?

A. It indicated the data came before March 7, 2016, 9:57 a.m.

MR. LOCKARD: If we can advance to the next slide?

Q. Now, Mr. Berger, there is about a one-minute window between the February 26, 9:36 a.m. commit that matched the file release by WikiLeaks, and then the next commit at 9:37 a.m. Can you just describe why it is that you chose to extend the window to the February 26th date instead of the March 1st date?

A. So after looking at the data and seeing that there was the duplicate commit value, I decided to take the more conservative approach. Instead of saying data had to have come after March 1st, I extended the window back and saying that no, the data had to come after February 26th in order to, again, have a more conservative approach to this analysis.

MR. LOCKARD: If we can look at the next page, please?

Q. Was there another file called solutionevents.CS in the Vault 7 release?

A. Yes.

Q. Did you perform the same type of analysis that you just described with the last file?

A. Yes.

Q. Did you calculate a hash value for this file?

A. I did.

Q. And is that reflected here on this page also?

A. It is.

THE COURT: May I interrupt for one quick second?

Just to let you know that all 15 of you have tested negative so you can rest easy.

You may proceed.

MR. LOCKARD: Excellent. Thank you, your Honor.

BY MR. LOCKARD:

Q. So I don't think there is need to read the long string of letters and numbers but if we can turn to the next page?

What is shown on this page?

A. So similarly to the previous file we looked at, this is a listing of commit date and times as well as the calculated hash values for the file solutionevents.CS.

Q. Was there an entry in that commit history that had the identical hash value as the file release by WikiLeaks?

A. Yes, there was.

Q. And when was that?

A. That was the entry on February 13, 2016, at 3:13 p.m.

MR. LOCKARD: If we can move to the next page?

Q. And again, do we have that analysis in timeline format?

A. Yes.

Q. So based on solutionevents.CS what did you conclude about the date range of the data released by WikiLeaks from Stash?

A. So since they disclosed the version committed at February 13th, 2016 at 3:13 p.m., that indicated the data came from a point in time after that commit. It also indicated the data came from a point in time prior to March 4th, 2016, at 9:45 a.m.

MR. LOCKARD: And if we can advance to the next slide.

Q. Is that the time period highlighted here?

A. Yes.

MR. LOCKARD: If we can advance to the next slide?

Q. What was your overall conclusion combining those two date ranges?

A. So when we combine the date ranges we have a time period of February 26, 2016, 9:36 a.m. through March 4th, 2016, at 9:45 a.m. of when the data disclosed by WikiLeaks from Stash came from.

Q. And as we saw again with the Marble.horig file, you could have selected a window between March 1st and March 4th?

A. Correct.

Q. Just remind us why you chose the window of February 26.

A. Trying to maintain a conservative approach to the analysis.

Q. Mr. Berger, did you review just these two files or did you review additional files?

A. I reviewed additional files.

Q. Approximately how many files did you review in conducting your analysis?

A. A few dozen, probably.

Q. And why did we focus on these two files in your testimony today?

A. So we focused on these two files because they represent the files that are closest together on the timeline. There were other files that indicated a window that was much larger, this is much more concise.

Q. Did you identify any files that were inconsistent with this conclusion?

A. I did not.

MR. LOCKARD: If we could go to the next page?

Q. Can you give us an overview of how you conducted your timing analysis for the Confluence data?

A. So with Confluence I had to take a slightly different approach. Because of the way Confluence works and data from the Confluence system is displayed and calculated in real-time, every time a user goes to the page, there weren't exact copies of files that I could use to hash and look for identical copies from the WikiLeaks disclosures. In addition, as Mr. Leedom had testified based on the flaw in the backup script and the work that WikiLeaks would have had to have done to modify or re-render the data to make it displayable on their website, again, every tiny little change would throw a hash match as being completely useless.

Q. So how did you use version control to conduct your timing analysis for Confluence?

A. So Confluence has, again, a similar version of version control. It keeps track of every time you update a page, it saves that particular page, and it has all the previous versions of that page. In the data that WikiLeaks disclosed from Confluence, they actually included the most recent version of a Confluence page as well as all the previous versions of that page.

MR. LOCKARD: So if we can turn to the next page of Exhibit 1704?

Q. Is this an example of what you were just describing?

A. Yes.

Q. Is this one of the pages that you analyzed in your timing analysis?

A. Yes, it is.

Q. So were you able to identify a corresponding page in the Confluence backups?

A. Yes, I was.

MR. LOCKARD: Let's turn to the next slide.

Q. How are you able to identify a corresponding page in Confluence?

A. So we took the number that's indicated there that ends in 129 and I look for that in the Confluence database. The results were that that was the unique ID for a specific page that had several different versions of the page in the database.

MR. LOCKARD: And can we turn to the next slide, please?

Q. Can you tell us what is reflected here?

A. So this is a listing of modifications to the Confluence page entitled Michael R.'s home.

Q. And if you look at the column that is circled prevver -- P-R-E-V-V-E-R -- was there relevant information in that column?

A. Yes, there was.

MR. LOCKARD: We can turn to the next slide.

Q. What was the relationship between that Confluence data and the WikiLeaks data?

A. So the way that WikiLeaks published the data, they named the page with the -- and they embedded the prevver number into the name of the HTML file on their site.

Q. So if we can turn to the next slide, please?

Can you describe the version history for Michael R.'s home from Confluence?

A. So the query we are looking at here came from a backup of Confluence from April 25th, 2016, and as shown on the screen at that time there is 17 previous versions of that page.

Q. And if we can turn to the next slide? How many versions of this page were there in the WikiLeaks release?

A. In the WikiLeaks release they released the primary page that we are looking at here, and they also had links to 16 previous versions.

Q. So which version are we looking at as the main page from the WikiLeaks release?

A. We are looking at the 17th release on WikiLeaks.

Q. If we can turn to the next slide? What is the date that that 17th version was saved to the Confluence backups?

A. That was saved on March 2nd, 2016, at 3:58 p.m. local time.

Q. So if we can turn to the next slide? Is that that same information represented in timeline format?

A. Yes, it is.

Q. And what conclusions were you able to draw from that information?

A. That the data that WikiLeaks disclosed came from data saved after March 2nd, 2016, at 3:58 p.m.

Q. And if we can advance to the next slide? As highlighted here?

A. Correct.

Q. Let's look at the next slide, please. What are we looking at on this page?

A. So this is another page that was part of the WikiLeaks disclosure entitled Build Felix LP.

Q. If we can advance to the next slide? Did you find a corresponding page in the Confluence backups?

A. I did.

Q. And advancing again to the next slide, please? Were you able to confirm that these pages matched?

A. Yes.

Q. And how were you able to do that?

A. By looking at the page, specifically the content that was disclosed by WikiLeaks and looking at the actual page data from the Confluence database backup.

Q. So you didn't rely just on the matching page number and prevver number?

A. No.

MR. SCHULTE: Objection.

THE COURT: Overruled.

Q. I'm sorry, Mr. Berger.

A. No, I did not rely just on those values.

Q. If we can look at the next slide, please? And what was the version history of this page Build Felix LP?

A. So in the database that I analyzed there were 15 versions of the page saved.

Q. And advancing to the next slide, how many versions of the Build Felix LP page were there in the WikiLeaks release?

A. So on the main page for Build Felix LP there were links to seven previous versions, indicating this was the eighth version of the page.

MR. LOCKARD: If we could advance to the next slide?

Q. What did that indicate about the relevant dates for your timing analysis?

A. That indicated that the data had to have come after March 2nd at 8:01 a.m. and prior to March 3rd at 6:47 a.m.

Q. And advancing to the next slide, so here we are back at the timeline for Michael R.'s home. If we can build in that new data on the next slide, please? So combining that information, were you able to draw conclusions about the date range of the data from Confluence that was released by WikiLeaks?

A. Yes.

Q. And what was that conclusion?

A. That the data that was disclosed by WikiLeaks came from a window between March 2nd, 2016 at 3:58 p.m. and March 3rd, 2016 at 6:47 a.m.

MR. LOCKARD: And if we can advance to the next slide?

Q. The window highlighted here?

A. Correct.

Q. Did you combine the timing analysis from your Stash analysis and your Confluence analysis?

A. I did.

Q. If we can advance to the next slide, please? And one more? What was the window that you derived from those two combined analyses?

A. So again, the Confluence window was a smaller window but it fit within the larger window generated by the Stash analysis.

Q. Mr. Berger, were you able to identify a Confluence backup that fell within that window?

A. I was.

Q. If we can advance to the next slide? What is shown in these two directory listings?

A. So this is a listing of the two parts of the Confluence backup, on the left are the SQL files from the data and on the right are the compressed archives of the home directory.

Q. And if we can advance to the next page? Which backup fell within the window indicated by your timing analysis?

A. That would be the March 3rd backup.

MR. LOCKARD: If we can advance to the next slide?

Q. In your review of the data information for the Confluence backups, did you observe anything unique about those two backup files?

A. I did.

Q. What was unique about the two backup files?

A. The access time was noticeably different.

Q. Different in what way?

A. The other backup files were created and modified within minutes of each other, essentially the backup script would create them, they would be finalized and saved to disk, and then never looked at again. The March 3rd backup files both had a date accessed approximately a month and a half after they were created and the access time on each of those was one minute within each other.

MR. LOCKARD: Next slide, please.

Q. Were you able to review data information associated with the March 2016 Stash backups?

A. I'm sorry. Can you repeat that?

Q. Were you able to review any data information associated with March of 2016's Stash backups?

A. I was not.

Q. Why is that?

A. They had been deleted.

MR. LOCKARD: If we could advance to the next slide? If we could turn to page 77 of the slide deck?

Q. So, Mr. Berger, we looked at the April 20th, 2016 access date for the March 3rd Confluence backups. Did you review the defendant's user activity after April 20th, 2016?

A. I did.

Q. And looking at this e-mail from Government Exhibit 1305-5, what did you learn from this e-mail?

A. I learned that on Sunday, April 24th, 2016, the defendant ordered a USB to SATA adapter.

MR. LOCKARD: If we can look at the next slide?

Q. What date is reflected here or what information is reflected here from Government Exhibit 1306-1?

A. These are the details of the defendant's purchase I just mentioned.

Q. And what is the item description?

A. The description is an Inateck USB 3.0 to SATA dual bay USB 3.0 hard drive docking station.

MR. LOCKARD: If we can look at page 79?

Q. What is the picture that is shown here?

A. That is a picture of the item the defendant ordered.

Q. Is it the item or an example of the item?

A. It is an example of the item, it is not the actual item that the defendant procured.

Q. So what is a SATA drive?

A. So a SATA is a common interface used on hard drives in the computing industry. USB is a much more common interface that many people are familiar with. In order to take an internal hard drive, which is designed for being installed inside a computer that has a SATA interface and connected to your computer, through a USB port you would need some type of adapter. The device shown here would serve that purpose. There would be a USB cable that comes out of the back of the device and plugs into your computer and then you would take a SATA internal hard drive and essentially drop it down into the slots on the top, kind of like a toaster.

Q. So you describe SATA drives as being internal drives?

A. Correct.

Q. Are there other types of external storage that are more commonly used?

A. Yes, there are.

Q. What is the difference between a SATA drive and a DVD or a thumb drive, for example?

A. So DVD drives are limited at much lower capacity than SATA again USB drives are also limited, although they have come quite a way in the last few years, however the cost for the same amount of storage on a thumb drive is much higher than a standard internal hard drive.

Q. And if we can turn to page 80? What is reflected here from the defendant's Google search history derived from Government Exhibit 1305-7?

A. So these are additional searches the defendant performed on April 24th, as well as pages that were visited by the defendant.

MR. LOCKARD: If we could, Ms. Cooper, if we could please pull up Government Exhibit 1207-41? And if you can expand the top three or four lines?

Q. So Mr. Berger, you testified about the difference in storage capacities between SATA drives and other types of external storage?

A. Correct.

Q. What is the approximate size of the Confluence and Stash backups from early 2016?

A. The Stash backups shown here would be approximately 200 gigabytes.

Q. Do you recall the approximate size of the Confluence backups in March of 2016?

A. They were significantly smaller, I believe in the order of tens of gigabytes.

Q. Now, on Friday you testified about your review of digital data relating to secure deletion techniques?

A. Yes.

MR. LOCKARD: If we could look at page 93 of the 1704? Thank you, Ms. Cooper.

Q. You testified about a utility called Eraser Portable?

A. Yes.

Q. Remind us, what is Eraser Portable used for?

A. Eraser Portable is a utility to securely erase files.

Q. And is this a timeline representation of the activities with Eraser Portable that you testified about on Friday?

A. It is.

Q. Beginning with opening the Eraser Portable utility on April 23rd of 2016?

A. Correct.

Q. And then can you just briefly summarize what happened between April 23rd and April 28th?

A. So between that time the defendant added two folders and securely erased those folders, those were named Brutal Kangaroo and Array List. After that time the defendant added five files named data2, data3, data4, data5, and data6.bkp to the queue to be securely deleted, however he terminated the Eraser program before actually securely deleting those files.

MR. LOCKARD: Ms. Cooper, if we could look at page 95 of the slide deck?

Q. You also testified about the downloading of a utility called DBAN or Darik's Boot and Nuke?

A. Correct.

Q. Can you describe the purpose of that utility?

A. That is a utility that you can boot up off of so you are not using your computer's primary operating system and it can easily wipe, in a secure fashion, all the drivers on your system.

Q. And what is the date that the defendant downloaded that wiping utility?

A. April 30th of 2016.

Q. Mr. Berger, are you familiar with hard drives that were recovered from the defendant's apartment in March of 2017?

A. Yes.

Q. And if you can, I think, look behind you on the floor there should be Government's Exhibits 1608, 1609, 1610, 1611, 1612, 1613, and 1614, and 1615.

A. There are.

Q. Could you pull up some of those hard drives so that we can see them?

A. So this is 1608 and 1609.

Q. And what type of hard drive is 1608?

A. 1608?

Q. Yes, sir.

A. It is an internal SATA hard drive.

(Continued on next page)

MR. LOCKARD: Ms. Cooper, if you could please turn to page 103 of the slide deck.

Q. Does this list the types of external hard drives that are with you up there on the witness stand?

A. It does.

Q. Mr. Berger, did you have an opportunity to review those hard drives for any data that was stored on them?

A. I did.

Q. And what did you find?

A. There was no data.

Q. And what, if any, conclusions were you able to draw from that?

A. They had been wiped.

Q. How did you know that they weren't reformatted?

A. There was no file system present on the drive. When you wipe a drive, it completely removes all data. In order to actually utilize the drive again, you would need to reformat it and create that file system or the table of contents we talked about on Friday.

Q. And about how many of those external hard drives are listed as additional hard drives?

A. Seven of them.

MR. LOCKARD: If we could please turn to page 59 of the slide deck.

Q. So, on Friday, Mr. Berger, you described WikiLeaks instructions to leakers about how to transmit data?

A. Correct.

Q. Including the use of the TOR network and the Tails operating system?

A. Correct.

MR. LOCKARD: If we could turn to page 72.

Q. And can you remind us what the defendant did on April 24 of 2016?

A. He began downloading the Tails file.

MR. LOCKARD: If we could turn to 74.

Q. Again, what's reflected on this screenshot?

A. This is a screenshot of a Linux virtual machine that was found on the defendant's desktop computer and contained within the virtual machine. On the virtual machine desktop was TOR browser.

Q. And according to WikiLeaks, what are the purposes of Tails and TOR?

MR. SCHULTE: Objection.

THE COURT: Sustained. I think we've covered that.

MR. LOCKARD: If we could turn to page 101, please.

Q. Looking at the defendant's Google history on May 1, 2016, Mr. Berger, can you please describe what's being searched for?

MR. SCHULTE: Objection. Asked and answered.

THE COURT: I don't think this has been, so I'll allow it.

Go ahead.

BY MR. LOCKARD:

Q. Again, this is from Government Exhibit 1305-8, the defendant's Google history from May 1, 2016, at 3:18 a.m. through 3:21 a.m.

Mr. Berger, what did the defendant search for at 3:18 a.m.?

A. So, 3:18 a.m., he searched for "how long does it take to calculate MD5," and he also searched for "how long does it take to MD5 a file" approximately nine seconds later.

Q. And what is MD5?

A. MD5 --

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. MD5 is a commonly used hashing algorithm.

MR. LOCKARD: If we could turn to page 105 of the deck.

Q. Mr. Berger, did you review the defendant's computer activity on April 30 and May 1?

A. I did.

Q. Can you describe what's shown here on this slide derived from Government Exhibit 1401-1?

A. This is a portion of what's referred to as the auth.log. It's a log file under Linux that deals with events relating to authentication. This is the auth.log from the Linux virtual machine that was found on the defendant's desktop.

Q. And did the auth.log contain data relevant to the use of the computer by the user?

A. Yes.

Q. Specifically what type of activity?

A. Events that showed the screen saver was unlocked.

MR. LOCKARD: If we could turn to the next slide.

Q. We see some unlocking activity at 10:04 and at 11:04 on April 30?

A. Correct.

MR. SCHULTE: Objection. Leading.

THE COURT: It is, but I'll allow it.

Go ahead. Just watch it going forward, Mr. Lockard.

MR. LOCKARD: Of course, your Honor.

If we could turn to the next slide.

Q. At what time does this particular sample of the auth.log activity pick up?

A. The log file portion that we're looking at starts at May 1 at 1:22 in the morning.

Q. And did you also review the auth.log entries between the morning of April 30 and the early morning of May 1?

A. I did.

MR. LOCKARD: If we could move to the next slide.

Q. Was there user activity on the evening of April 30 and the morning of May 1?

A. There was.

Q. And at what times was the virtual machine screen saver unlocked on May 1?

A. At 1:57 a.m., 2:34 a.m., 2:56 a.m., and 3:18 a.m.

MR. LOCKARD: If we can now please turn to page 111.

Q. Mr. Berger, we already talked about the external state of hard drives that were found in the defendant's apartment. Were there also internal hard drives in his home computer?

A. There were.

Q. And did you find evidence relating to data deletion on those internal hard drives?

A. I did.

Q. And can you just remind us again what is sort of the general setup of the defendant's home computer?

A. So, the defendant had four internal hard drives on the primary desktop computer. There was a single drive that served as the C drive, which is where the operating system was installed, and there were three additional drives that were combined to form what's known as a RAID volume or a RAID 5 array. That tick was known as the D drive on the computer.

Q. And just so we can understand a little bit better, how do three hard drives become a single D drive in the defendant's computer?

A. So, the drives connect to what's called a RAID controller. That essentially does the hard part, and it abstracts away that one drive is made up of three. It also allows for data security in that the way a RAID 5 works, if any of the three drives fails, your data is not lost. You replace it with an additional drive, and the RAID volume rebuilds. It's commonly used in environments where data reliability is an issue.

Q. And looking at the forensic artifact shown here on page 111, which is derived from Government Exhibit 1402-6, what does this artifact relate to?

A. This relates to the MFT file on the D drive.

Q. And what is the MFT file?

A. The MFT file is the master file table on the MTFS file system. It is quite literally a table of contents of the file system.

Q. And what were you able to learn from this information shown here on page 111?

A. That the MFT file was created on May 5 of 2016, at 8:01 p.m.

Q. And what does that reflect; what type of user activity does that reflect?

A. That reflects that the D drive was reformatted at that time.

MR. LOCKARD: If we could turn to page 112.

Q. So this page derived from Government Exhibit 1403-6, can you describe what this artifact relates to?

A. Similar to the prior artifact, this is the forensic details of the MFT file. This one is from the C drive, or the primary drive of the defendant's computer.

Q. And what type of hard drive was the defendant's C drive?

A. That was a Samsung SSD.

Q. What is an SSD?

A. SSD is a solid state drive. It indicates that unlike traditional hard drives that had moving parts there are no moving parts. All of the information is stored on internal bit sets.

MR. LOCKARD: If we could turn back to page 102.

Q. Looking at the defendant's Google search history on May 4 of 2016, what is that search?

A. On May 4, 2016, at 8:49 a.m., the defendant searched for "can you use DBAN on SSD?"

Q. Mr. Berger, can you wipe a solid state drive?

A. You can.

Q. Are there any concerns with wiping a solid state drive?

A. There are.

Q. What are they?

A. If you use a traditional wiping utility on an SSD, it causes excessive wear and tear based on how an SSD actually stores data internally. There are, in fact, separate mechanisms designed to wipe data from an SSD. Usually these involve some kind of utility from the drive's manufacturer.

MR. LOCKARD: If we can turn back to page 112.

Q. So here, with the defendant's C drive, the Samsung solid

state drive, what information did you learn about the master file table?
A. That it was created on May 5, 2016, at 11:15 p.m.
Q. And what does that indicate?
A. That indicates that the C drive was reformatted at that time.
Q. And how long after the D drive was reformatted was it that the C drive was reformatted?
A. I believe it was about three hours.
Q. Now, Mr. Berger, on Friday, you described the differences between reformatting and wiping a drive. What is the difference to a forensic investigator between reformatting and wiping?
A. So, reformatting, again, just re-creates that table of contents that we talked about, re-creates the file system. The underlying data on the drive is all still there. Since there's nothing actually pointing to it, the new file system would consider the area where that data is to be unallocated space, and if at any point in time it needs to utilize that space it will and it will overwrite the files. In that interim time, that data is still recoverable to anyone performing digital forensics on that system.
Wiping the drives would overwrite all of the available areas with zeroes or random data, essentially preventing forensic recovery of that data.

Q. Mr. Berger, in your review of the defendant's home computing equipment, did you find evidence of data that existed prior to the date of this format of May 5, 2016?

A. There was data that had downloaded and modified dates prior to that date, correct.

Q. Now, you talked about the use of Eraser Portable and those five backup files?

A. Yes.

Q. Was that prior to the date of this reformatting, May 5, 2016?

A. Yes.

Q. Did you find any artifacts relating to the five backup files when you reviewed the computer after May 5 of 2016?

A. I did not.

Q. And what, if any, conclusions are you able to draw from that?

A. That the drives had been wiped.

MR. LOCKARD: If we could turn to page 113, please.

Q. Mr. Berger, is this a summary of some of the events that you've testified about between Friday and today?

A. Yes.

Q. Is that shown in timeline format?

A. It is.

Q. Let's just walk quickly through this if we can.

What happened on April 20 of 2016, based on your investigation and your observation of Mr. Leedom's testimony?

MR. SCHULTE: Objection. Asked and answered.

THE COURT: I'll allow it.

A. The defendant copied the March 3 backups from DevLAN and with the same source of the data that was disclosed by WikiLeaks.

Q. Now, in this timeline there are a number of events in blue above the timeline and some events in gold below the timeline. Generally, what type of activity do the events in blue relate to?

A. The events in blue relate to data destruction.

Q. And the events in gold, what type of activity do those gold events relate to?

A. They relate to reading data from a drive and transmission of data.

Q. And I don't think we have to walk through each of these individually, but at the conclusion of those series of events relating to data destruction and data transmission, what happened on May 5 of 2016?

A. The defendant reformatted both drives on his computer.

MR. LOCKARD: Your Honor, may I have one moment?

THE COURT: You may.

MR. LOCKARD: No further questions, your Honor.

THE COURT: Thank you.

Cross-examination.

JUROR: Your Honor, can I use the restroom?

THE COURT: Sure. Let's take a pause for juror No. 13 to use the restroom that's here in the jury room.

Ms. Smallman, you can take him there.

If the rest of you want to stretch while we're waiting, you may do so.

All right. We are ready to proceed.

Mr. Schulte, you may begin when you're ready.

CROSS-EXAMINATION

BY MR. SCHULTE:

Q. Good morning.

A. Good morning.

Q. You testified on direct that you work for the FBI, correct?

A. Correct.

Q. The government did not hire a third-party expert for this investigation, correct?

A. I'm not aware of.

Q. The government basically asked itself to conduct a forensic examination, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Let's talk a little bit about the multiple hard drives and other electronics found at my home. All right?

A. OK.

Q. You didn't find any CIA hard drives at my home, correct?

A. I don't know the source of the hard drives that were found there, correct.

Q. Well, computers record the model and serial number of each hard drive, thumb drive or external drive inserted, correct?

A. They can.

Q. And you know from the CIA, they keep track of the serial numbers and purchase orders, correct?

A. I'm not aware of what the CIA keeps track of.

Q. So you didn't take the hard drives from my home and compare to see if any of them originated from the CIA?

A. I personally did not. I don't know what the other members of the investigative team did.

Q. OK. But to your knowledge -- I mean that would be a big finding if that had been the case, right?

A. I can't judge one way or the other. I just am not aware of that information.

Q. OK. So to your knowledge, you didn't find any CIA hard drives or thumb drives at my home, correct?

A. Again, I can't say one way or the other.

Q. I'm saying, to your knowledge, you didn't find them.

A. I'm not aware of any, no.

Q. Similarly, you found no evidence that any of my hard drives or moveable media what were ever connected to the CIA computers, correct?

A. I'm not aware of that, no.

Q. You found no model numbers or serial numbers on my CIA workstation that matched one of my personal drives, correct?

A. I'm not aware of any of that analysis, no.

Q. Specifically, you found no evidence that I copied the Vault 7 or Vault 8 data to my home computer, any of my devices, correct?

A. Specific evidence of those files?

Q. The question is you found no evidence that I copied the Vault 7 or Vault 8 data to my home computers, any of my devices, correct?

A. I did not find any specific forensic artifacts that indicate that, correct.

Q. No evidence that I stored Confluence of my home devices, correct?

A. I would not say no evidence. There was reference to a folder named Brutal Kangaroo.

Q. That has nothing to do with Confluence, though, right?

A. I believe there was a Confluence page for Brutal Kangaroo.

Q. OK. But you didn't find any evidence that I stored Confluence on my home devices?

A. I can't speak to what the contents of that Brutal Kangaroo folder was, so I can't confirm that, no.

Q. There's no -- you don't know what was in that folder,

right?

A. I don't, but it was named Brutal Kangaroo.

Q. OK. But you don't have any evidence that there was any Confluence data on my home device from the forensics, right?

A. Other than that one folder named Brutal Kangaroo, correct.

Q. Same for Stash, right?

A. Correct.

Q. No evidence of any Atlassian products from the CIA, correct?

A. Correct.

Q. No evidence of any of the CIA backups on my home devices, correct?

A. Correct.

Q. I want to briefly go through your timing analysis. What did you have access to in order to conduct your timing analysis?

A. I was giving -- I was given backup copies from both Confluence and Stash.

Q. And your timing analysis can only establish a lower bound, correct?

A. Incorrect.

Q. That's incorrect? A lower bound is essentially the first backup that contained the data released by WikiLeaks, correct?

A. Correct, data that was from a, the CIA system and was also identically present on WikiLeaks. Yes.

Q. OK. And you said that your analysis does not establish a lower bound?

A. I did not say that. It does establish a lower bound.

Q. I'm sorry. What did you disagree with then?

A. I believe I disagreed with something you mentioned about an upper bound.

Q. I'm sorry. I think then I must have mis-asked the question. The question should have just been about the lower bound, so let me --

THE COURT: All right.

MR. SCHULTE: Let me just make sure this is the right question?

THE COURT: Mr. Schulte, just keep your thoughts to yourself. Just ask a question, please.

MR. SCHULTE: OK.

Q. Just to make sure this is the right question. Your timing analysis can only establish the lower bound, correct?

A. Incorrect.

Q. OK. What's incorrect about that?

A. It established upper bounds, as I testified about.

Q. Oh, you're saying that it can establish an upper bound?

A. It can, and it did, establish an upper bound, as I testified about.

THE COURT: Can you just explain what you mean by a lower bound and upper bound?

THE WITNESS: So, my understanding of what he's asking is a lower bound and upper bound form a window of when the data disclosed was taken from. Without the presence of an upper bound, it could have only come from some point after a lower bound with no upper bound to cap that window.

THE COURT: By lower bound you mean the first date that it, the earliest time that it could have come from, and the upper bound is the latest time that it could have come from? Is that what you mean?

THE WITNESS: Correct.

BY MR. SCHULTE:

Q. OK. But your analysis -- let's take a look at your slide on No. 44. That's exhibit 1704. I'm having a little bit of issue pulling it up. OK.

OK. Slide 44. So all the data from WikiLeaks can be found in every single backup from March 3 through -- from March 3, 2016, through March 6, 2017, correct?

A. I can't confirm that, no.

Q. You didn't do -- that wasn't part of your analysis?

A. I did not look at every single piece of data in every single Confluence backup, no.

Q. OK. But you did confirm that -- if we look at slide 37; you did talk about version history, correct?

A. Correct.

Q. So all these versions, as you note here, it records all the previous version, right?

A. Correct.

Q. Slide 29, you notice the same thing here too, correct?

A. Correct.

Q. And then slide 15, you have commit date/times right here, correct?

A. Correct.

Q. So if you have this backup from March 7, 2016, at the end, right, you could go back to February 26, 2016? Correct?

A. Technically possible, yes.

Q. Well, it's very easy to do that in Git, correct?

A. Easier than Confluence, correct.

Q. OK. So you don't actually establish an upper bound; the data could come from later backups, correct?

A. I believe the upper bound is established by the disclosed -- the data actually disclosed on WikiLeaks.

Q. Right. But your analysis cannot determine what data WikiLeaks actually obtained, correct?

A. Based on my analysis and reviewing Mr. Leedom's analysis, WikiLeaks disclosed -- they went to great lengths to disclose all the data they had, including data that was internally marked deleted in the system that they put on their site anyway. That would indicate that if there was existing data they had, they would have disclosed it thereby setting an upper bound.

Q. You're just speculating as to what WikiLeaks disclosed, correct?

A. That's not speculation.

Q. It's not speculation to say most likely you think that WikiLeaks disclosed this because they disclosed as much information as they could from that time period?

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. I would not call that speculation. I would call that offering my expert opinion.

Q. OK. But just from a forensic standpoint, it is conceivable that WikiLeaks could track the March 2, March 3 version from a much later backup, correct?

A. A forensic standpoint would require a forensic artifact, so I'm not sure what you're asking.

Q. Is it conceivable, therefore, that WikiLeaks could track the March 2, March 3 version from a much later backup?

A. In order to only disclose certain data from a later backup? Is that what you're asking?

Q. I'm asking if a later backup, if WikiLeaks could track the March 2, March 3 version from, say, a March 10 backup?

A. It might be possible, but they would need to have a reference point, from what I understand.

THE COURT: Can you just explain what you mean by that?

THE WITNESS: Essentially, they would need to have a copy of the March 3 backup to know exactly how the data was stored at that point in time. If something might have been deleted and actually expunged from the database, they might not have that in a much later backup.

THE COURT: So in other words, WikiLeaks could have used a later backup but it would also have needed to have the March 3 backup to see what the data, how the data was on that date? Is that what you're saying?

THE WITNESS: Yes, based on my understanding and my understanding of Mr. Leedom's analysis, correct.

BY MR. SCHULTE:

Q. But the database would record the dates just like this, the dates and times for when files are changed, correct?

A. It records when, in this case, in Stash, when files are committed, correct.

Q. The same thing exists in Confluence, the database actually records when the files are changed, right?

A. Yes.

Q. OK. So the database keeping track of when files are changed, as long as you have the database, you can select which files you want, correct?

A. Again, there's no guarantee that a later database would have all of the preexisting data from a previous point in time.

Q. But that -- you're basing that simply because there was the analysis that the databases were corrupt, correct?

A. No. I'm basing that on my knowledge of how databases work and how the systems work and that something could have been removed from the system, and there's no guarantee that that -- it would be in a later version of the backup.

Q. Yes, sir. But if a file is deleted, that file is still preserved in the version history, right?

A. In Confluence, yes, deleted files are still in the database. However, I don't know that there's not a mechanism to actually expunge a deleted file from the Confluence system.

Q. OK. So you've done no analysis to determine whether later backups actually expunge data from previous backups, correct?

A. I did not. I don't recall performing that analysis, no.

Q. OK. So, if that analysis turned out that no data was expunged, then any later backup would contain all the previous iterations, right?

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. If no data was expunged from the system, then yes, theoretically, a later backup would have all the previous backup to date or the previous data to date.

Q. OK. So why was no analysis of that performed?

A. I can't answer that question.

THE COURT: Meaning you're not permitted to answer the question, or you just don't have an answer?

THE WITNESS: I don't have an answer. I just have the work that I was assigned to look at.

THE COURT: So you weren't asked to perform that analysis.

THE WITNESS: Correct.

BY MR. SCHULTE:

Q. So this slide No. 11 is inaccurate then, is it not?

A. I don't believe so, no.

Q. If your slide is based solely on your timing analysis that you performed, it should simply say WikiLeaks disclosed information from up to March 2, 2016, correct?

A. In my opinion, this slide is accurate.

Q. The question was if you're basing it solely on the forensic timing analysis that you performed, your forensic analysis simply concluded that WikiLeaks disclosed information from up to March 2, 2016, right?

A. The forensic analysis I performed created a -- established a window of when that data was from. This slide is based on both my forensic analysis and my overall understanding of other analysis performed in the investigation.

Q. But you don't actually know whether WikiLeaks received an official backup file or from a file pulled from the Stash and Confluence virtual machines directly, right?

A. It's my understanding based on the, again, the analysis and testimony of Mr. Leedom, that they would have had to receive a backup copy in order to re-create and render the data as they did.

Q. So your analysis is based on Leedom's analysis, is that correct?

A. My opinion of what WikiLeaks disclosed is, yes.

Q. OK. But forensically, you can't say whether or not WikiLeaks received a backup from the offsite backup, correct?

A. I was not part of any analysis looking at offsite backups. I'm not aware of how they were stored or access control or anything like that.

Q. OK. But you don't know if WikiLeaks received every single backup off DevLAN, correct?

A. I can't speak to that one way or the other.

Q. OK. And you don't know if WikiLeaks received every byte of the data off DevLAN, correct?

A. Again, I can't speak to that one way or the other.

Q. OK. So all you can say is WikiLeaks disclosed information from up to March 2, 2016, right?

A. March 3, 2016, correct.

Q. Well, I mean there was no data from March 3; it was just March 2 was the latest in your analysis, right?

A. I don't remember if there was anything from the actual morning of March 3 that we looked at, so I --

Q. OK.

A. I don't remember.

Q. All right. Let's move on to slide 51.

You testified about my Google searches on April 15, correct?

A. Correct.

Q. At 2:43 p.m. on April 15, I'm at work, right?

A. I would think so.

Q. And at this time I'm an Atlassian administrator, correct?

A. On April 15, yes, you were.

Q. And that includes Confluence, correct?

A. Yes.

Q. So it's my job to check on access controls and ensure Confluence is running smoothly, correct?

A. I don't know what your specific job roles entailed.

Q. Well, as an administrator for Confluence and applications, that's what an administrator would do, right?

A. Yeah, those are some of the tasks an administrator might be performing. Yes.

Q. OK. Which includes locking down pages, correct?

A. In terms of restricting access to others on a particular page?

Q. Yes.

A. It might be, yes.

Q. All right. Slide 52, you note April 18, 2016, I conducted searches for copying files across Linux servers, correct?

A. Correct.

Q. And to be clear, this requires you to have access to both the servers, right?

A. You would need access to the source location where you're copying from as well as a destination where to put the file, correct.

Q. OK. And through your investigation, you learned that I administered multiple Linux servers at the CIA, correct?

MR. LOCKARD: Objection. Form.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. As part of your investigation, you knew that my job entailed administering multiple Linux servers at the CIA, correct?

MR. LOCKARD: Objection. Form.

THE COURT: Overruled.

A. I'm aware that your job did involve administrating certain systems, yes.

Q. OK. And I also wrote malware for the CIA, correct?

A. From my understanding, yes.

Q. Including Linux malware, correct?

A. I don't recall the specifics or ever being told the specifics of the types of malware you worked on.

Q. Well, that would be important for your analysis, would it not?

A. In what way?

Q. Well, if I -- if I'm working on Linux tools for copying data, that would explain the Google searches, correct?

MR. LOCKARD: Objection to form.

THE COURT: All right. Let's just ask a new question, please.

Mr. Berger, you answer. He asks the questions. You don't ask him questions.

Let's ask a new question, Mr. Schulte.

MR. SCHULTE: OK.

Q. So knowledge of specifically what type of software I'm writing would be relevant to what Google searches I would be running, correct?

A. It could be, yes.

Q. OK. And as a general rule, you knew through your investigation that most of the software written was focused on exfiltrating large quantities of data, correct?

A. I was not aware of that, no.

Q. OK. But these searches are conducted while I'm at work, correct?

A. I believe April 18, 2016, was a Monday and they were during what I would consider normal business hours, but I can't confirm whether you were actually at work at that time.

Q. OK. 53, these searches are programming-related searches, correct?

A. They're related to hashing algorithms, which could be used in programming, correct.

Q. I visit specifically multiple programming websites, correct?

A. It appears that way, yes.

Q. Programmers.stackexchange.com, correct?

A. Correct.

Q. And I think one of the searches that you didn't identify on direct here at 11:39 a.m. is specifically searches for FNV-1ACplusplus, right?

A. Correct.

Q. What is C++?

A. It's a programming language.

Q. OK. And that's the programming language that I used to write malware at the CIA, correct?

A. I can't confirm that, but it wouldn't surprise me.

Q. And there's a visit to cplusplus.com, correct?

A. Yes.

Q. And again, writing hashing algorithms is obviously part of my job at the CIA, correct?

MR. LOCKARD: Objection. Form.

THE COURT: Overruled.

A. It could be.

Q. OK. I'm going to pull up what's already in evidence as Government Exhibit 407.

So start and end dates there are from April 2016 to June 2016, correct?

A. That's what it says, correct.

Q. And this is -- this shows my name at the top, correct?

A. It does.

Q. OK. And the narrative here for the work that was being done during this period, it specifically mentioned thumb drive collection tools, correct?

A. It would seem to indicate that, yes.

Q. Tools to siphon data from various thumb drives and insert it into target computers, correct?

A. Yes, that's what it says.

Q. In which case fast hashing algorithms are critical to ensure the integrity of the collection, correct?

A. Yes.

Q. And it's also critical to ensure that you do not re-collect the same files and waste time, correct?

A. That would be a wise decision, yes.

Q. OK. So these searches would reflect those types of issues, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. So these searches were related to what I was working on at the CIA during this time, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Let's move on, please.

BY MR. SCHULTE:

Q. All right. As part of your investigation, you familiarized yourself with the workings of WikiLeaks, correct?

A. Yes.

Q. You did that to assist with your work on this case, correct?

A. Yes.

Q. And through that analysis, you discover that WikiLeaks tries to protect identities of persons leaking information, correct?

MR. LOCKARD: Objection. Form.

THE COURT: Overruled.

A. Yes, based on their instructions.

Q. And you know what data WikiLeaks released from the CIA, correct?

A. Yes.

Q. But you don't know how much data it actually received, correct?

A. I do not have access to WikiLeaks' servers, no.

Q. OK. So starting on slide 54, during your direct, you describe WikiLeaks transmission instructions, correct?

A. Correct.

Q. And I believe you testified that these are WikiLeaks pages from April 23, 2016, correct?

A. Correct.

MR. SCHULTE: I'd like to pull up what's in evidence as Government Exhibit 1351.

Q. According to my Google searches, between 2006 and July 2016, I only visited the WikiLeaks website once, correct?

A. Correct.

Q. And that was in 22 -- I'm sorry -- 2010, correct?

A. I don't have the date for that particular search in front of me.

Q. Sorry. Let me scroll.

It's from 2010, correct?

A. Yes, that's what this indicates.

Q. OK. So of course, I would not have seen this page from 1704, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Well, there's no forensic evidence to support any theory that I viewed the WikiLeaks website in April or May of 2016, correct?

A. There's no forensic artifact showing that you visited WikiLeaks, correct.

Q. OK. Let's talk about TOR now.

TOR is run by the Electronic Frontier Foundation, correct?

A. I'm not sure if they run it or if they just advocate for its use.

Q. Well, the EFF is a well-respected nonprofit organization, correct?

A. From my understanding, yes.

Q. And it advocates for privacy and security, correct?

A. Yes.

Q. The U.S. State Department used to fund TOR, correct?

A. I'm not aware of that.

Q. Well, you are aware that TOR was created by the U.S. government, correct?

A. I am aware it was initially created by a part of the U.S. government. I'm not aware of what part, though.

Q. OK. And Facebook makes itself available over TOR, correct?

A. I can't speak specifically to Facebook. However, I do know certain companies do offer TOR-facing websites.

Q. The New York Times uses TOR, correct?

A. I can't speak to that.

Q. Well, many, many news organizations use TOR, right?

A. I believe so, but again, I can't speak to specific knowledge of that.

Q. You didn't do research through this case into TOR?

A. I did some research, and I also was familiar with TOR prior to this investigation.

Q. OK. And you learned through this investigation that TOR browser here was installed on this Linux Mint VM, correct?

A. Correct.

Q. But the TOR browser was actually installed in October of 2015, correct?

A. I don't recall the date that the browser was installed in the VM.

MR. SCHULTE: OK. Let's pull up -- I'm just going to show to the witness and the parties what's been marked as defense exhibit 1409-1.

Q. Do you recognize this kind of output?

A. It would appear to be text about --

THE COURT: Don't state what is there. Just do you recognize this?

THE WITNESS: I don't recognize this, no.

MR. SCHULTE: OK. I think at this time I might read in a stipulation, 3006.

THE COURT: Any objection?

MR. LOCKARD: No objection.

THE COURT: You may proceed.

MR. SCHULTE: Can the government pull that up? I don't think I have a copy of it.

THE COURT: Why don't you just skip the first paragraph, since the jury's heard that several times.

MR. SCHULTE: OK.

THE COURT: You can display it to the jury just so they can follow along.

MR. SCHULTE: "If called as a witness, a representative of Verizon Communications with knowledge of the matter would testify that defense exhibits 201 through 208 are true and correct copies of records from Verizon, which were mate at or near the time by, or from information transmitted by, a person with knowledge of the matters set forth in the records; they were kept in the course of a regularly conducted business activity; and it was the regular practice of that business activity to maintain the records.

"If called as a witness, a representative of Amazon.Com Inc. with knowledge of the matter would testify that defense exhibit 209 is a true and correct copy of a document from Amazon from records associated with Amazon user account joshschulte1@gmail.com, which were made at or near the time by, or from information transmitted by, a person with knowledge of the matters set forth in the records; they were kept in the course of a regularly conducted business activity; and it was the regular practice of that business activity to maintain the records.

"If called as a witness, a representative of Meta Platforms Inc. with knowledge of the matter would testify that DX10 is a true and correct copy of Facebook records associated with Facebook username pedbskball, which were made at or near the time by, or from information transmitted by, a person with knowledge of the matter set forth in the records; they were kept in the course of a regularly conducted business activity; and it was the regular practice of that business activity to maintain the records.

"If called as a witness, a representative of Plex Inc. with knowledge of the matter would testify that defense exhibit 211 is a true and correct copy of records from Plex associated with Plex user account joshschulte1@gmail.com, which were made at or near the time by, or from information transmitted by, a person with knowledge of the matters set forth in the records; they were kept in the course of a regularly conducted business activity; and it was the a regular practice of that business activity to maintain the records.

"If called as a witness, a representative of Google LLC with knowledge of the matter would testify that defense exhibit 301, 301-1, 303-1, and 303-2 are true and correct copies of records from Google associated with Google user account joshschulte1@gmail.com, which were made at or near the time by, or from information transmitted by, a person with knowledge of the matters set forth in the records; they were kept in the course of regularly conducted business activity; and it was the regular course -- practice of that business activity to maintain the records.

"It is further agreed that the stipulation, Government Exhibit 3006, may be received in evidence as a government exhibit at trial."

OK. I'm going to show just the witness and the parties what's been marked as defense exhibit 1409.

Q. Do you recognize this, sir?

A. Not this particular document. It appears to be information about files.

Q. You know what the data represents, right?

MR. LOCKARD: Objection.

THE COURT: Do you recognize the data? Do you know what this file is?

THE WITNESS: It seems like it's some type of metadata listing, information about files.

THE COURT: But you don't know where it comes from or what it is?

THE WITNESS: Not just looking at this, no.

BY MR. SCHULTE:

Q. Are you certain that this is not a document that you created? It may help looking at the top.

A. OK. That -- that does help. I don't recall creating this file. I'm -- I don't remember, but it appears to be a listing of the decrypted contents of the home directory from that virtual machine.

MR. SCHULTE: I move to introduce just a subexhibit of this.

THE COURT: I don't know what that means, Mr. Schulte.

MR. SCHULTE: Just the small, just one part of that exhibit I want to introduce.

MR. LOCKARD: Objection.

(Defendant conferred with standby counsel)

THE COURT: Sustained. Lack of foundation.

MR. SCHULTE: All right. Back to just 1409 then. I move to introduce this.

MR. LOCKARD: Objection. Relevance. Foundation.

THE COURT: Sustained on foundation.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. Well, through your forensic examination of the virtual machine, you conducted directory listings of those drives, correct?

A. I reviewed listings of files in forensic software, yes.

Q. So part of forensic investigation entails obtaining directory listings, correct?

A. If you mean generating a report, like a single file that lists every file, generally it's not something we do all the time. We would look at files and folders within the confines of the forensic program itself.

Q. Through forensic analysis you wouldn't get a listing of all the files and review that data?

A. We might, but generally, we're not going to look at a single listing of all the files because it's going to be exceedingly voluminous and very large. Usually within the forensic program itself, we could look at either specific folders, subfolders, or look at the entire file system but create filters for certain types of files or attributes.

Q. OK. So your forensic analysis software basically helps you interpret this data, right?

A. Correct.

Q. OK. But the forensic tools that you would use, such as FTK, would allow you to export file listings, correct?

A. Correct.

Q. And file listings, and there were -- let me rephrase.

And you generated file listings for the different drives from the virtual machine, correct?

A. I don't recall if I generated file listings for each of the drives as a separate export from the forensic program.

Q. OK. Does this exhibit refresh your recollection about generating those listings?

A. As I said, it appears to be a listing of files from your home directory on the virtual machine, but I can't recall if I was the one who generated the listing.

Q. Even if you can't recall generating it, these are the listings, right?

A. It would appear to be a file listing from the -- from the

Josh home directory on the virtual machine, correct.

MR. SCHULTE: OK. Now I move it into evidence.

MR. LOCKARD: Objection. Foundation.

THE COURT: Overruled. Admitted.

(Defendant's Exhibit 1409 received in evidence)

MR. SCHULTE: Can I publish it to the jury, defense exhibit 1409? I just want to highlight row 1844.

Q. Do you recognize this listing?

A. It appears to be the item for the TOR browser on your desktop.

(Continued on next page)

BY MR. SCHULTE:

Q. And the dates on these, what year do you see on these?

A. I see 2015.

THE COURT: Can you just explain what those dates would reflect in the file listing from the home directory?

THE WITNESS: So I don't know the details because they weren't displayed.

THE COURT: Speak into the microphone.

THE WITNESS: I don't know the details of the date because it wasn't indicated, but a file listing would usually have created modified less access dates. So it would appear that that was one of those dates but, again, from just that exhibit I couldn't tell which was being indicated.

THE COURT: Just a reminder, when you say this came from the virtual machine from the defendant's computer at his home, can you just explain, again, what that means?

THE WITNESS: Sure. So they're on the defendant's desktop computer. He ran Windows, and within Windows he had a virtual machine that was Linux. This is a screenshot of the desktop of that virtual machine so it is, again, a computer within a computer. So within the virtual machine he had a home directory like you might have a home directory on your Windows computer. So that was a listing of the files -- appeared to be a listing of the files from the home directory.

THE COURT: Just for the record, this was page 74 from the slide deck 1704, and so just to make it even clearer, if the date on the file listing was from 2015 it is your opinion that that means that the TOR browser on the virtual machine was either created, modified, or accessed in 2015; is that correct?

THE WITNESS: Correct.

BY MR. SCHULTE:

Q. This is nearly a year before the events in April 2016, correct?

A. I believe it was the fall of 2015 so it would have been maybe about six months; but before, yes.

Q. And, in fact, you don't note on your PowerPoint presentation but when was this Linux Mint VM meant to be created?

A. I don't recall the date.

Q. All right. I will just show the witness what's been marked as Defendant's Exhibit 1404-1. Do you recognize what type of document this is?

A. It appears to be some kind of log file from a Linux system.

Q. And you reviewed log files in your forensic examination of the virtual machine, correct?

A. Correct.

Q. And one type of log file that you would have reviewed was something known as sys log, correct?

A. I can't recall specifically but it's a common file that -- it would have been a common file to review for Linux forensic analysis.

Q. And what types of information would the sys log file show?

A. It would show various events relating to the underlying system or the kernel of the operating system.

Q. And through your analysis you would have exported the -- you exported these log files, correct?

A. I can't recall exporting them. If I was conducting analysis within a forensic program I would, if I came across an artifact that was interesting, I would generally bookmark it within the forensic program. It is possible I might take a screenshot, it's possible I exported it, but I can't recall if I did export a sys log file.

Q. What creates the sys log file?

A. It's created by the system.

MR. SCHULTE: I move for this 1404-1 into evidence.

MR. LOCKARD: Objection. Foundation.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. We at least established -- let me rephrase.

The TOR browser install in 2015 would suggest that the VM was created at least at this time, correct?

A. It would suggest that, yes.

Q. So the Linux Mint VM from 1704, slide 74, is at least from the fall of 2015 creation time, correct?

A. It would appear that way, yes.

Q. Through your forensic examination of that virtual machine you discovered that it was used regularly from October 2015 until May 2016; correct?

A. I don't remember the specific analysis in terms of usage patterns but it was used, I believe, up until early May of 2016.

Q. Publish to the jury and move on to slide 71 and Tails. Through your forensic examinations you discovered that DevLAN had Tails and many other Linux distributions, correct?

MR. LOCKARD: Objection. Form.

THE COURT: Sustained as to form. It is a compound question, Mr. Schulte.

Q. Through your forensic examination you discovered that DevLAN had multiple Linux distributions, correct?

A. I'm not aware of what Linux distributions they had. Again, my analysis primarily focused on the evidence recovered from your apartment.

Q. But it would have been important to your analysis to determine what types of things I worked on at the CIA, right?

A. Again, I believe early on in the investigation we were given some information. Again, sitting here today I don't remember exactly what types of tools you worked on other than what has already been looked at here.

Q. But you said in general you knew that I did work on Linux-based tools, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Next question.

Q. Well, you learned that it was normal behavior for CIA malware developers to download and test new Linux distributions, correct?

MR. LOCKARD: Objection. Form.

THE COURT: Overruled. But before you answer that question, can you just explain what a Linux distribution is?

THE WITNESS: So the way Linux operates, it is an open-source community that they release what is known as the Linux kernel, it is the underlying -- the kernel is the underlying component of an operating system. Different developers have, over the years, taken the underlying, basically guts of what Linux is and they create their own Linux distributions so they will package up a fully operational operating system that you can download and different distributions will have different additional software, some might be only command line based, some might have graphical interface, there will be different graphical interfaces so there is many Linux distributions out there that you can download and use.

THE COURT: Mr. Schulte, do you want to just ask your question again now?

MR. SCHULTE: Yes.

BY MR. SCHULTE:

Q. Just to clarify that, Tails is one of many Linux distributions, correct?

A. Correct.

Q. So you learned through your investigation that it was normal behavior for CIA malware developers to download new Linux distributions, correct?

MR. LOCKARD: Objection. Form.

THE COURT: Overruled.

A. I don't recall learning that specific fact, no.

Q. So for testing Linux tools you would need Linux to test against, right?

A. Of course.

Q. So it would be normal to download Linux distributions if you are writing tools for those, right?

A. Yes.

Q. And because there are so many different, what they call flavors of Linux, it is important to download as many of them as you can, right?

A. It would depend on what your goal is, what your purpose, if you were writing software for specific distributions or if you were trying to write software for as many distributions as possible.

Q. And if you are writing software for Linux and you want it to be used by as many people as possible, you would want to test on as many different platforms, right?

A. Of course.

Q. The same for other operating systems like Windows or Mac, right?

A. It would be fair to say you would want to test against any possible software that your software would run on, yes.

Q. And your forensic analysis didn't stand-alone, correct?

A. I'm not sure which particular part of the analysis you are talking about.

Q. I am talking in general now, you relied on Leedom's analysis too, right?

A. For my opinion, correct.

Q. And you relied on other data, correct?

A. Correct.

Q. And you wanted to know if my searches and behavior were work-related; right?

A. Correct.

Q. OK. Through your investigation -- forensic investigation you learned that I regularly -- I regularly downloaded updated Linux distributions, correct?

MR. LOCKARD: Objection. Form.

THE COURT: Overruled.

A. I don't recall that specific fact now.

Q. Through your investigation did you not discover additional downloads of Tails?

A. I believe there was one additional download of Tails that I can recall, yes.

Q. So in your slide 72 you note that Tails 2.2.1 was downloaded on April 24th, 2016, correct?

A. Correct.

Q. But you didn't include a slide about the download of 2.5 Tails on August 9, 2016; correct?

A. Correct.

Q. I am going to show the witness what is marked as Defendant's Exhibit 1405. Do you recognize this type of document?

A. It appears to be a metadata listing for a file.

Q. Through your forensic tools, those will give you what is called forensic artifacts, correct?

A. Correct.

Q. And forensic artifacts are just essentially pieces of data that you discover through the analyses, right?

A. Essentially, yes.

Q. And specifically this type of analysis will give you information about files, correct?

A. Correct.

MR. SCHULTE: I move to introduce Defendant's Exhibit 1405.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 1405 received in evidence)

BY MR. SCHULTE:

Q. And this is a forensic artifact showing Tails version 2.5, correct?

A. It appears that way, yes.

Q. And this torrent was created July 31st, 2016; correct?

A. Correct.

Q. And then a week or so later I downloaded it on August 9, 2016; correct?

A. It appears that way, yes.

Q. And there is no evidence that I ever re-booted my computer to use Tails, correct?

A. That's correct.

Q. There is no evidence that I created a Tails VM, correct?

A. That's correct.

Q. So there is no evidence that I actually used Tails, correct?

A. Correct.

Q. I want to talk about data storage and will pull in what is admitted as Government Exhibit 1605-3. From your investigation you reviewed multiple electronic devices from my apartment, correct?

A. Correct.

Q. Including these servers, right?

A. Correct.

Q. And these servers ran multiple virtual machines, correct?

A. I believe so. I remember looking at the servers early on so about five years ago now, but that -- I seem to recall there were additional virtual machines on the servers, yes.

Q. And these virtual servers ran multiple different services, correct?

A. I don't recall what specific services they ran.

Q. But you recall in your analysis public storage, correct?

A. I don't recall that, no.

Q. You don't recall the krypton.org website?

A. I do recall that website. I don't recall specific features or services that were made available.

Q. You don't recall public shares from that server?

A. I do not.

Q. I am going to show what's been marked as Defendant's Exhibit 212. You did, through your analysis, you did learn about a service called Plex, correct?

A. I seem to recall that, yes.

Q. And Plex is a service for streaming videos or TV shows; right?

A. That's my understanding, yes.

Q. And through the Plex service you can share this data with other individuals, correct?

A. To my understanding, yes.

Q. And people can add content, correct?

A. I am not aware of the specifics about what users can add content.

Q. But you were aware that there were multiple users that logged in, accessed the Plex server; right?

A. I remember hearing about that, yes.

Q. All right. Take that down.

I am going to move on to slide 110. So before we begin discussing too much of the forensics, I think you testified on direct something about wiping or re-formatting a computer, correct?

A. Correct.

Q. But there is no forensic evidence that supports your conclusion that a system was wiped instead of newly installed or upgrades, correct?

A. Incorrect.

Q. That's incorrect. OK. What is your evidence?

A. Specifically, the artifacts from the Eraser Portable analysis, the five data.bkp files that indicated they were present on your D drive. At one point in the analysis I did try different recovery techniques to look for those files and nothing was present and found on the D drive that would indicate that those drives had been wiped prior to the drive being re-formatted, more than likely.

Q. But your analysis can't determine if there wasn't a wipe but simply an upgrade to new drives, correct?

A. Correct.

Q. Because you testified that I had a RAID 5 system, correct?

A. Correct.

Q. I'm going to pull up Government Exhibit 1601-16.

This is a picture of the RAID 5 setup, correct?

A. It peers to be that way, yes.

Q. So you testified RAID 5 requires at least three drives, correct?

A. Correct.

Q. And it stripes data across all those three drives, correct?

A. Correct.

Q. And adds a parity bit for data integrity, correct?

A. Correct.

Q. And the RAID 5 system works in such a way that a single drive can fail and there is no data loss, correct?

A. Correct.

Q. You can simply take out the defective drive and slap in a new one, correct?

A. Correct.

Q. And you are aware that you cannot increase the capacity of a RAID 5 system, right?

A. Under standard RAID 5, correct.

Q. And so Government Exhibit 1601-18, this shows the RAID controller configuration on the computer, correct?

A. Yes. It appears that way.

Q. You can only delete the RAID or create a new RAID, correct?

A. I believe so, yes.

Q. So if you wanted to add hard drives to a RAID 5 you have to create a new RAID 5 system, right?

A. Yes.

Q. Alternatively, if you want to create a RAID 5 when you don't already have one that is going to require a whole new install, right?

A. If you are talking about if you wanted to create a new RAID array, I'm not sure what you mean by install.

Q. I'm saying if you have a system with a single drive and now you want a RAID 5 system, right, you have to create a whole new RAID system because it doesn't exist, right?

A. Well, you would be creating a RAID array from where there wasn't one before, yes.

Q. And that process of creating a RAID system is going to destroy everything on the drive, right?

A. If you are referring to using the existing drive that you are replacing with a RAID array, if you inserted that drive into the newly created array it would essentially destroy the contents of that drive, yes.

Q. So it would be important that you copied everything off the drive before you created the -- before you included that in the RAID system, right?

A. If you wanted to preserve what was on there, sure.

Q. As part of your forensic investigation you learned that during the first week of May every year I performed upgrades on many of my computers and servers, correct?

MR. LOCKARD: Objection. Form.

THE COURT: I don't think it is a form objection but the objection is sustained.

Q. As part of your investigation you wanted to learn my pattern of work, correct?

A. My initial investigation was more concerned with just the technical analysis of the evidence.

Q. That technical analysis would depend upon normal user activity, right?

A. It could. Yes.

Q. So it would be important, through your investigation, to go back over history of drives and determine timelines, correct?

A. I'm not sure what you mean by timeline of drives. Throughout the investigation if we -- anything that we uncovered or any artifacts we were in constant communication with the special agents, the investigators, we shared that information with them and they would have been the ones, if they needed to go out and, you know, if they wanted to go interview you or talk to you, they would kind of ascertain that information, we were just focused on analyzing the data.

Q. Well, I mean, through the forensics you can determine when new drives were added or when new servers are brought online, this type of information, right?

A. To some extent, yes.

Q. So through that investigation you learned that I yearly upgraded systems, right?

MR. LOCKARD: Objection.

THE COURT: You may answer. Overruled.

A. I was not aware of that, no.

Q. But back to the RAID 5. Once again, upgrading a RAID 5 system with new larger drives requires a new install, right?

A. If you are replacing an existing RAID 5 volume with a new drive to increase the capacity, yes, that would require replacing the drives and recreating the raid array.

Q. And so thus creating the RAID 5 system from scratch, right?

A. Correct.

Q. And neither of these is a wipe or re-format, right?

A. Not in the general sense.

Q. It's a new install, right?

A. When you create the RAID array it initializes the drive and sets up how the data is going to be striped across the drives and then presents that to the operating system as a single logical volume that you could format or do whatever you want to.

Q. And the facts and forensic evidence clearly supports the notion that the RAID 5 system was newly created in May of 2016, correct?

A. It does not.

Q. And why do you think that?

A. The forensic evidence shows that the RAID volume was re-formatted in May of 2016.

Q. How can you show that it is re-formatted instead of newly installed?

A. I'm not saying it was installed or it was not a newly installed. I'm saying the forensic artifact shows that it was re-formatted.

Q. I guess I'm not following. If it is not -- how do you know it is a re-format instead of doing it the first time?

A. The drive was formatted in early May.

Q. OK.

A. We can tell that by the forensic artifact I already testified about.

Q. OK, but this --

THE COURT: Just to clarify, I don't know if this is what Mr. Schulte is getting at but when you say it is formatted, can you determine if that is formatted for the first time, i.e. that the drive was created in early May or it is formatting or reformatting an earlier existing drive? Can you determine that from the forensics?

THE WITNESS: Not from that artifact, no.

BY MR. SCHULTE:

Q. Were there any artifacts that you could use to determine whether this was a new RAID 5 system?

A. I don't believe so, no.

Q. So the question, going back to the question, the forensic evidence -- so you are testifying the forensic evidence doesn't support a conclusion one way or the other. Is that what you are saying?

A. One way or the other about -- I'm not sure what you are asking.

Q. Of whether the RAID 5 system was newly created or whether there was an existing one that was re-formatted.

A. Again, the forensic artifact only indicates that the drive was formatted. At that point it does not indicate whether it was an existing RAID array or a pre-existing RAID array, or an existing RAID array or a new RAID array.

Q. I wish to show just the witness and parties a sub-exhibit Defendant's Exhibit 302-1.

Do you recognize this type of data displayed here?

A. It seems to be in a similar format as a results of Google searches that were returned.

MR. SCHULTE: I move to introduce this into evidence.

MR. LOCKARD: Objection. Foundation.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. All right. Let's just pull up the Government Exhibit of the Google searches, I guess. So if we pull up Government

Exhibit 1305-1, I just want to highlight this column 19674. Can you see that?

A. Yes, I can see the row indicated 19674, yes.

Q. And this search is conducted May 1, 2016; right?

A. Yes.

Q. And the UTC time is 20:36, right?

A. Correct.

Q. So that would have been 4:30 Eastern Time, right?

A. Yeah, 4:36 Eastern Daylight Time; correct.

Q. And what is the search there?

A. The search was for best way to store user data.

Q. And then the next search after that?

A. RAID 5 or data backup.

Q. We are going to skip these -- and then the visit here -- or the search here? I'm sorry.

A. The search was for RAID performance comparison, Intel RAID controller.

Q. And then the next page that is visited, it is from extremetech.com, right?

A. Yes.

Q. It is looking at RAID performance, correct?

A. It appears to be the name on the article of that site, yes.

Q. And the next as well, foxdeploy; right? Foxdeploy.com?

A. Yes.

Q. And that's also looking at Intel RAID performance, correct?

A. It would appear that way. It is entitled: Windows v. Intel RAID Performance Smackdown.

Q. And just to be clear, we are talking about RAID performance, we are talking about essentially the performance of the RAID system in general, right?

A. Correct.

Q. So this would be, like, drive speed, right?

A. It's one aspect of how well your RAID will perform, yes.

MR. SCHULTE: And based on that, now I move to introduce the sub-exhibit 302-1.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 302-1 received in evidence)

BY MR. SCHULTE:

Q. So around May 1 it is clear from the searches that there is research into RAID 5 systems, right?

A. There is research about RAID 5 or RAID performance, yes, or RAID performance. I don't remember if it specifically said RAID 5.

Q. Well, here we can highlight this exhibit here. Specifically it is RAID 5 or data backup, right?

A. Yes.

Q. So essentially this type of search is trying to determine whether to use RAID 5 or backup data, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Q. OK. From the technical standpoint, what is your understanding of this type of search to mean?

A. It could mean that you are looking at how to back up a RAID 5 volume. It could mean that you are looking to look at some other data backup solution or RAID 5 as a backup solution. There is several different ways you can interpret that search.

Q. Did you not think that search was related to RAID 5 or backup in general would have been relevant as to this time frame?

A. I believe they were relevant.

Q. And as part of your investigation you discovered the precipitating event to these Google searches about backups and RAID systems, right?

A. I'm not sure what event you are referring to.

Q. Well, my NAS failed during attempts to upgrade it during this time, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Ladies and gentlemen, let me remind you, again, that the questions that Mr. Schulte asks of any witness are not evidence, it is just the witness' testimony that is evidence. A question can be asked by either side in a way that suggests that there is information behind it but it is not the question that is the evidence so do not assume anything from any question. You may rely only on the witness' answer for the evidence.

New question, please.

BY MR. SCHULTE:

Q. Through your forensic examination you determined -- or you discovered that my NAS failed during this time frame, right?

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. I do not recall that, no.

THE COURT: What is "NAS" a reference to?

THE WITNESS: It stands for Network Attached Storage. It is a device that can contain several hard drives; you would plug it into your network and you can access it over the neck for storing files.

BY MR. SCHULTE:

Q. Through your forensic examination you discovered that there was a public NAS for private data storage, correct?

A. I do not recall that, no.

Q. You saw references to network storage in your forensic examination though, correct?

A. Correct.

Q. And during this time you recovered forensic evidence that one of my network storage arrays failed, correct?

A. I do not recall that, no.

Q. Well, if a network storage array fails it would be important to salvage the data from that, correct?

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. Yes, if it were possible.

Q. And then you would want to set up some new array to store that data, right?

A. If that's what your goal is, if you wanted to re-establish that data and it's availability, yes.

Q. Let's move on, slide 76 in your presentation. You talk a lot about SATA adapters when you testified in your presentation, correct?

A. It was mentioned, yes.

Q. A SATA adapter does not connect to a network, correct?

A. I can't say for certain that there aren't SATA adapters that have network connectivity. In this particular case the SATA adapter did not have network connectivity.

Q. But you a SATA adapter is not used to transfer data across the Internet, right?

A. Not by itself, no.

Q. In fact, the item I purchased is not even a SATA adapter, is it?

A. It is a SATA adapter, it translates the SATA interface to a USB interface. Technically speaking it could be viewed as more of a docking station than an adapter.

Q. So you would agree, from a technical standpoint, the name of this type of device is really a docking station; correct?

A. It is a docking station based on just its physical appearance but I believe it is still technically accurate to describe it as a SATA adapter.

THE COURT: We are going to break there for break.

Ladies and gentlemen, you know the drill. Don't discuss the case, keep an open mind, don't do any research about the case. With that, it is 11:40, so let's be prepared to pick up again at 12:20 so please be ready to go at 12:15 when Ms. Smallman will come get you.

With that, enjoy your small breaks. Thank you.

(Continued on next page)

(Jury not present)

THE COURT: Mr. Berger, you are free to step down. Because you are on cross you may not communicate about the substance of your testimony with anyone from the government side so please don't speak with them, certainly about the subject of your testimony. Please be back in the courtroom or in the witness room at 12:15 ready to go. Thank you.

THE WITNESS: Understood.

THE COURT: Mr. Schulte, any estimate of how much longer you have on cross?

MR. SCHULTE: Yes. So that was an issue I wanted to bring up, Judge.

I provided to the government a lot of forensic artifacts that the witness created -- or forensic artifacts that the government turned over in discovery. So I provided the government these exhibits and I have been trying the last week or so to see if the government would agree to stipulations on these. To the degree that the government is not going to agree to stipulate to its own discovery as provided to me in its expert's own artifacts as provided to me, it could take a substantial time to get through all of those forensics if I am going to be fought on admitting them at every step of the way.

THE COURT: Well, I would certainly urge the government, if those things are indeed artifacts or analyses or spread sheets or data that this witness created or would be in a position to know, I certainly think it might speed things along to either acknowledge that or stipulate orally and consent to their admission. So, too, if there is an exhibit -- an example 301-1, which I take was an extraction of data of what is already in evidence as Government Exhibit 1305-1, if it is apparent that that's the case, I think it would speed things along if we can just agree to that and admit it. That being said, I don't know if the government was in a position to confirm that. And, if not, then it was necessary to go through the steps as laying proper foundation.

So the bottom line is, government, I would certainly urge you to look at them and if we can speed things along, great. If not, obviously Mr. Schulte does need to lay a proper foundation to admit things and we will proceed. So mindful of that, I guess how much have you gotten through of what you have for Mr. Berger?

MR. SCHULTE: So I'm on page 15 of 29 of my cross, so.

THE COURT: Very good. And assuming we get to another witness, who is up next, Mr. Lockard?

MR. LOCKARD: Mr. Weber will be next.

THE COURT: One housekeeping note. The stipulation 3006 referenced a bunch of underlying exhibits, none of which have been admitted. I don't know if, Mr. Schulte, you intended to offer them, but I just wanted to note that.

MR. SCHULTE: Yeah, they're coming in. I mistakenly thought one of the exhibits would be in there but it is coming in -- they're coming in in this cross anyway.

MR. LOCKARD: So that stipulation is an authenticity and business records stipulation. We maintain relevance and hearsay objections to some of those so we will just take it as it comes.

THE COURT: OK. I noted that it did not stipulate to their admission so I figured there might be some issue and I guess we will take it as it comes but I just wanted to make sure we were all on the same page.

Anything to discuss before you take your breaks? Mr. Lockard?

MR. LOCKARD: Not from us, your Honor.

THE COURT: Mr. Schulte?

MR. SCHULTE: No.

THE COURT: And reminder, government, I will ask for an update of the transcript of Friday's proceeding at the close after lunch hoping that you have resolution on that and, if not, certainly by the end of the trial day.

Thank you. Please be back in the courtroom by 12:15 and enjoy your breaks.

(Luncheon recess)

(Continued on next page)

AFTERNOON SESSION

12:15 p.m.

(Jury not present)

THE COURT: You may be seated.

Let's get Mr. Berger back on the stand.

Government, any report on the transcript?

MR. DENTON: Yes, your Honor.

Two things. First, with respect to the transcript, we've had a chance to review it. There are no issues. So the transcript from Friday, we have no applications with respect to redactions.

THE COURT: Great. I don't know how the logistics of this work, but will Mr. Schulte have one before he returns to the MDC?

MR. DENTON: I would assume it will be fine for him to just take the hard copy that was provided, but otherwise, we can make sure that Mr. Hartenstine knows whatever he needs to know about how that should be handled.

THE COURT: Great.

MR. DENTON: The second issue is, your Honor, we were just provided at the break with a whole slew of new defense exhibits, including a variety that Mr. Schulte apparently intends to use with this witness. We obviously have a continuing objection to the belated production. There's some extent to which we understand that trials are dynamic and require ongoing productions, but to the extent that we are just getting these for the first time now, we object to the defendant introducing them.

MR. SCHULTE: I think majority of those are just sub-exhibits for the Google searches that -- they should have been provided before, but I don't know what happened. Somehow they didn't get them. But I think that was the majority of the new stuff, just sub-exhibits from the Google searches.

THE COURT: When you say sub-exhibits, you mean extracted from the government exhibit Google searches that's already in evidence?

MR. SCHULTE: Yes. So if the government wants, I can pull it up on their exhibit and then introduce the subject of it. But it's just a simple thing of searching and finding the search results from there.

THE COURT: All right. If that's the case, I don't see any prejudice. Although certainly I don't want rolling productions of things that could have been produced earlier, trials, indeed, are dynamic.

MR. DENTON: I think with respect to those, your Honor, understood. I think there are a number of other exhibits that give us some concern, including things that the defendant has labeled expert presentations and other extremely large spreadsheet files from his home computer, which, again, gives us some pause about other aspects of his home computer that we need to treat with some sensitivity. Again, we can take these case by case, but I think there are at least some of those to which we think there's prejudice with the production.

THE COURT: All right. I guess we'll have to take it as it comes, I think, but duly noted and understood.

All right. The jury should be coming up in a minute. Anything else before they arrive?

All right. Sorry. One thing I wanted to ask. Am I correct that the next witness is subject to the courtroom-closure procedures? Is that correct?

MR. LOCKARD: That is correct, your Honor.

THE COURT: All right. Assuming we get there today, then my intention is to excuse the jury, tell them that I just have to handle some technical matter, probably excuse them to the jury room here so that they can stretch, use the restroom, and in the meantime, we can implement the restrictions.

All right. The jury should be here any second.

(Continued on next page)

(Jury present)

THE COURT: You may be seated. Welcome back, ladies and gentlemen. I hope you enjoyed your break.

We will continue with the cross-examination of Mr. Berger.

Mr. Berger, you may remove your mask, and you remain under oath.

Mr. Schulte, you may proceed.

BY MR. SCHULTE:

Q. OK. Before we pick up where we last left off, I just have a few questions for you. You met with the government to prepare your testimony, correct?

A. Correct.

Q. You had meetings with Mr. Lockard in his office, correct?

A. Correct.

Q. You met with him multiple times, correct?

A. Correct.

Q. How many times did you meet with him?

A. It was several over the last two to three weeks.

Q. More than ten?

A. I don't believe so.

Q. More than five?

A. Probably somewhere between five and ten.

Q. OK. Did you meet with him on Friday after you began your direct testimony?

A. I saw him in the -- in the office, yes.

Q. Did you speak with him over the weekend?

A. No.

Q. During these meetings, you discussed your testimony, correct?

A. Correct.

Q. You discussed what questions you would be asked, correct?

A. Correct.

Q. And how you would answer those questions, correct?

A. It wasn't discussed how I would answer. I gave my, what my answer would be to the questions posed.

Q. So practicing, basically, right?

A. To some extent, yes.

Q. And during those meetings, you reviewed the government's exhibits, correct?

A. Some of them, yes.

Q. And discussed how you would describe those exhibits to the jury, correct?

A. Correct.

Q. And you didn't meet with me before your testimony, correct?

A. I did not.

Q. You didn't speak with me over the phone, correct?

A. I did not.

Q. And you didn't review my exhibits, correct?

A. I believe one or two exhibits were shown to me.

Q. OK. So let's pick back up on 1704, slide No. 79. OK? I think we were discussing this device, and the correct name for this device is a hard drive docking station, right?

A. That's what's in the item description, yes.

Q. OK. And this type of device is typically used for what's called an off-line clone, correct?

A. That's one use for it.

Q. In fact, Amazon even markets the off-line clone right there in the description, correct?

A. Yes, correct.

Q. An off-line clone is a copy of a drive, correct?

A. Correct.

Q. And literally off-line, meaning it has nothing to do with the internet, right?

A. No. Off-line means that it doesn't have to be connected to a computer. You can use this device, from my understanding, plug it into power, and clone one drive to another without having hooked up to a computer.

Q. OK. But this device doesn't connect to the internet, correct?

A. Not to my knowledge.

Q. It has two slots for hard drives, correct?

A. Correct.

Q. And as you said, specifically this device is utilized to perform a complete forensic copy of one drive to another,

right?

A. I don't know if I'd use the term "forensic," but it would be safe to say it creates an exact copy, yes.

Q. OK. So if a hard drive is failing, this device would be ideal for trying to copy as much data as possible from the failing drive, correct?

A. It's one -- it's one way of doing it, yes.

Q. OK. And slide 79, you make much out of the same-day delivery, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. You testified on direct about the same-day delivery for this device, correct?

A. I don't believe that I did.

Q. OK. Well, through your investigation, you discovered I was an Amazon Prime member, right?

A. I don't recall that.

Q. Amazon Prime members receive free shipping, correct?

A. Yes.

MR. SCHULTE: I'll show just the parties what's been marked as defense exhibit 209-1. 209 is in evidence pursuant to a stipulation. 209-1 I'm showing to the witness.

Q. Do you recognize this output?

MR. LOCKARD: No objection to 209-1.

THE COURT: All right. Let's just admit it then.

(Defendant's Exhibit 209-1 received in evidence)

BY MR. SCHULTE:

Q. From the shipping, do you note how many of these are same day or discounted shipping?

A. If going by the "our shipping" column, looks like two items were charged for shipping.

Q. And then do you see the discount?

A. Yes, I do.

Q. So those were nullified by the discount, correct?

A. If that's how the -- if that's what the spreadsheet represents. Again, I'm not familiar with what every column in here means, but if the discount is the reduction of the "our shipping" or the total cost, then yes, it's safe to say that those would be free shipping as well.

Q. OK. And that device, that purchase was for a pillowcase, I believe, right?

A. Seems that way.

Q. OK. And then --

THE COURT: To your knowledge, are these purchases from Amazon?

THE WITNESS: I have no way of knowing that -- oh, it says Amazon confidential, so it's my understanding they would probably be from Amazon.

BY MR. SCHULTE:

Q. So January 19, portable air compressor, tire inflater purchased, right?

A. Correct.

Q. Portable PSI pancake compressor, right?

A. Yes.

Q. Emergency flashlight purchased, right?

A. Yes.

Q. OK. And in fact, if we go down, we see the device, the docking station purchased here on April 24, correct?

A. Yes.

Q. And this relates to your slide presentation, right; this is the same device?

A. It appears that way, yes.

Q. OK. And then if we go to September 21, 2016, we actually see the same device purchased again, correct?

A. It seems that way, yes.

Q. And that's the exact same device, right?

A. I can't say that without looking at the actual Amazon item number, but the description seems extremely similar, if not identical.

Q. OK. And that one was purchased same day too, right?

A. Looks that way, yes.

Q. OK. And the shipping was discounted on that, right?

A. It seems that way, yes.

Q. But you didn't include that purchase in your slides, correct?

A. I did not.

Q. OK. You don't think it's relevant to know for showing history?

A. In terms of a history of all of your purchases at Amazon, the specific item was selected because of its relevance within dates to other activities.

Q. Well, I mean isn't it relevant to the fact that it's purchased a second time in September; isn't that showing regular activity?

MR. LOCKARD: Objection.

THE COURT: Sustained.

MR. SCHULTE: OK. Next I want to show the witness what's been marked as defense exhibit 29-2.

Q. Do you recognize this kind of output too?

A. Seems similar format as the previous slide.

MR. SCHULTE: I move to introduce this one as well.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 29-2 received in evidence)

BY MR. SCHULTE:

Q. This is from Amazon as well, right?

A. Seems that way, yes.

Q. And these are purchases of tech devices, right?

A. Seems that way.

Q. OK. There is a purchase in February 2016 for a USB hub, right?
A. Correct.
Q. There's a purchase for a microSD card, correct?
A. Correct.
Q. And in fact, here, June 27, there's a purchase of a hidden camera pen, correct?
A. Correct.
Q. There's a purchase of SD cards, correct?
A. Correct.
Q. And solid state internal drives, correct?
A. Correct.
Q. And even external drives, correct?
A. I'm sorry. If -- if you said external or internal?
Q. External.
A. I --
Q. I'm sorry. You're right. Internal. I'm sorry.
A. Yes, there's an internal hard drive on line 203.4.
Q. OK. And memory, there's a purchase for memory, correct?
A. Correct.
Q. That's for upgrading your computer with more RAM, right?
A. It could be used for upgrading, or it could be used for building a new computer.
Q. OK. So during this time frame through 2016, there's lots of purchases for electronic devices, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

MR. SCHULTE: OK. I want to pull up what's in evidence as admitted exhibit 1601-2.

THE COURT: Is this Government Exhibit 1601-2?

MR. SCHULTE: Government Exhibit 1601-2.

Q. Do you recognize this?

A. Yes, that's a computer, I believe, recovered from your apartment.

Q. This was my home desktop, right?

A. I believe so.

Q. OK. So in your presentation, you wanted to imply that the docking station was used to transmit data, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. If someone were going to connect a hard drive to a computer, you would not need a docking station, right?

A. It would depend on the type of hard drive.

Q. OK. Well, let's look at Government Exhibit 1601-3. It also depends on your computer, right?

A. Correct.

Q. This is the back of the home computer, correct?

A. Correct.

Q. And can you tell the jury what these red ports are on the computer?

A. It's hard to see, but I believe that says they're eSATA ports.

Q. And those are used to connect the hard drive, right, to the back of the computer? Right?

A. You would need -- well, again, depending on the hard drive, an internal SATA drive would still need an adapter cable to go from internal SATA interface to an eSATA or external SATA interface. In addition to that, you would also need a power supply for your computer -- I'm sorry, a power supply for the hard drive.

Q. OK. But if you have SATA ports, those are much faster than the USB, right?

A. I believe they are faster than even USB3. How much faster over USB3, I'm not sure.

Q. OK. Well, based on the input here to the computer, you would not need to buy a docking station to connect the drive, right?

A. If you wanted to connect an internal SATA hard drive to this computer without a docking station?

Q. Yes.

A. You would -- you would still need some type of adapter. You would need to go from internal to external SATA, and you would need some kind of power supply to power the hard drive while it's connected. The docking station connects both of those sources of connectivity.

Q. OK. But you could use, instead of a USB, you could use a SATA adapter instead, right?

A. You could use an adapter to go from the internal SATA port on the hard drive to the external SATA port that's been shown there, the red port, but you would need that adapter, yes.

Q. OK. I'd like to go back to your presentation here, 1704. So on slide 81, you stated that I researched secure deletion programs, correct?

A. Correct.

Q. You did not provide a slide showing any research, right?

A. I believe that was indicated by the Google searches.

Q. The Google searches -- I'm talking about the programs, like Eraser Portable.

A. No, there's no slide that indicates you were researching Eraser Portable, correct.

Q. I mean any kinds of programs that are wiping specific files. Right?

A. I don't believe so, no.

Q. OK. If we go to Eraser Portable, slide 87, you said that I was testing Eraser Portable, right?

A. Yes.

Q. Do you know what portable apps are?

A. Yes.

Q. Portable apps are installed on removable media, right?

A. Generally, yes.

Q. Portable apps are used when you are traveling, right?

A. It's possible.

Q. Well, essentially, when you're using other computers, other than your typical ones, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. OK. There's VLC portable apps, right?

A. I'm sorry. Could you repeat that?

Q. There is a VLC portable app, right?

A. I'm not aware of it.

Q. But generally, you don't install portable apps on your home computer, right?

MR. LOCKARD: Objection.

THE COURT: I'll allow you to answer it.

Go ahead.

A. Generally, the designation "portable" indicates that you would install it to some kind of removable media, and then you could run the program on a computer without installing the program on that computer.

Q. OK. Through your forensic examination of DevLAN, you learned that portable apps were used in malware, right?

A. I was not tasked with investigating, forensically investigating DevLAN. Again, my analysis was mostly limited to the evidence recovered from your apartment. The exception is the evidence in DevLAN I reviewed regarding to the actual data that was leaked as well as the databases containing permission-change evidence.

Q. OK. But the work I was doing at the CIA would be relevant to your investigation, right?

A. To some extent, just, you know, as far as that, you know, what you were doing, that you were a software developer working on tools, yes.

Q. OK. But also specifically with respect to [redacted] [redacted], right?

A. I'm not sure what you mean by that.

Q. Do you know what [redacted] is?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Do you know that malware uses [redacted]?

MR. LOCKARD: Objection.

THE COURT: Can I see the parties at sidebar, please.

(Continued on next page)

(At sidebar)

THE COURT: Can you elaborate? I don't know if it's a general relevance objection or if there's a sensitivity here that I might not be aware of.

MR. LOCKARD: I think it's both. I think there's a relevance objection. It also appears to be that Mr. Schulte intends to suggest that his use of Eraser Portable was related to specific work that he was doing at the agency to develop specific tools or to specific operations, and this is not something that we've been given Section 5 notice of.

MR. SCHULTE: I mean the -- in general, the research and stuff that I'm doing at home as it relates to developing malware, it's what's going on, but there's no specifics -- I'm not tying any specific operation or anything. [redacted] is a general term, as is malware, as is [redacted] [redacted] Eraser Portable. So I'm just trying to introduce generically how malware uses [redacted] [redacted] and then tying in the fact that as a malware developer, this is normal research for malware. But I'm not trying to tie it into anything specifically to the CIA.

THE COURT: Unless there's evidence in the record suggesting that you were working on these things, which I assume would be classified and there was no Section 5 notice with respect to, how do you tie it to this case? This is just an abstract people who do malware do these kinds of things which involves this kind of program. There's no nexus to this case.

MR. SCHULTE: The nexus is that these type of testing that's being done on the application is consistent with malware developers testing functionality and use.

THE COURT: But unless you can prove that you were actually working on this, it's not sufficient to just state in the abstract that people who do malware might use this kind of program, and the specific question of whether you used it is not something that was noticed. So I don't see how you -- I'm not going to let you just float the abstract possibility to the jury that calls on them to speculate whether this was the kind of malware that you were involved in working on at the CIA, and to the extent that you want to elicit that it was the malware that you were working on at the CIA, that, I think, is classified, and I don't believe that there was any notice of it.

MR. SCHULTE: I mean I don't think that using Eraser Portable [redacted] would be something classified --

THE COURT: No.

MR. SCHULTE: -- they could then tie it to anything specific. That's all.

THE COURT: The point is I think that unless there is evidence in the record that suggests that you were working on the malware that you're trying to connect Eraser Portable to --

MR. SCHULTE: Right.

THE COURT: -- it has no relevance.

MR. SCHULTE: Oh, no. I do intend to introduce the specific types of tools I used. That's going to be like Bartender. It was already -- Bartender was discovered in 2015, [redacted], [redacted]. So it's already been outed. So there's no classification with Bartender and Eraser Portable.

MR. DENTON: That is flatly incorrect.

MR. SCHULTE: There's a specific classification of Bartender that's been outed in 2015 and the fact that [redacted] Eraser Portable?

MR. DENTON: First of all, Bartender was not outed.

THE COURT: Was not what?

MR. DENTON: Outed.

A malware tool was identified that was not connected to the CIA, and in fact, one of the things Mr. Schulte is charged with attempting to disclose is that connection. So first of all, the idea that Mr. Schulte's unaware of this classification issue is absurd. But secondly, there was extensive discussion about the parameters of what sorts of tools and what sorts of details about tools were permissible, and this is well beyond that.

THE COURT: All right. I agree. I also think, for what it's worth, that this is not the proper witness to even do this through, because he testified that his role did not involve reviewing what was on DevLAN, let alone what work you were doing on DevLAN. So to the extent that it's admissible at all, it would be through another witness or through your own testimony, and we can debate at a later time whether there was proper notice given to that. But the bottom line is you can't go there with this witness.

(Continued on next page)

(In open court)

THE COURT: All right. You may proceed, Mr. Schulte.

BY MR. SCHULTE:

Q. All right. Moving on to slide 91, you're a computer scientist, correct?

A. Correct.

Q. You're familiar with ArrayLists, right?

A. I am.

Q. ArrayLists are simply a fundamental data structure, correct?

A. Correct.

Q. Can you explain, you know, what ArrayList is to the jury?

A. So, data structures in computer science are a way of storing data in different ways. There's many different types of data structures. Different data structures are better suited for storing different types of data, sorted data versus unsorted data.

In computer science, arrays are one type of data structure. That ArrayList is essentially an implementation of a way of storing data using an array in a list-type format.

Q. It's a way to organize, store, and retrieve data, correct?

A. Correct.

Q. Knowing how to build and use data structures is part of a basic tool kit for every programmer, correct?

A. Correct.

Q. Data structures are like a hammer and a saw to a carpenter, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. OK. So ArrayLists is nothing -- ArrayList is computer science 101, correct?

A. Correct.

Q. There was nothing suspicious about that, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Well, there would be no nefarious reason to securely delete ArrayLists, correct?

A. Just by, again, the folder, this designates that a folder named ArrayList was deleted. It's impossible to know the contents of that folder.

Q. OK. So on that same token, as part of this investigation, you've heard of Brutal Kangaroo, correct?

A. Correct.

Q. And Brutal Kangaroo was the name of a project I developed at the CIA, correct?

A. That's my understanding, yes.

Q. And as far as you know, I was working on some aspect of Brutal Kangaroo from home, correct?

A. I have heard reference to that, I believe, earlier in the investigation, yes.

Q. And then bringing code snippets into the office from home, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. OK. Would it be possible for somebody like me to be working on aspects of projects at home and then taking it into the office?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Mr. Schulte, please keep your voice down when conferring with standby counsel.

BY MR. SCHULTE:

Q. Through your investigation, were you aware of CIA policy concerning taking software from the internet onto DevLAN?

A. I don't know the specifics of any particular policy.

Q. OK. So in your review of DevLAN, you discovered multiple code snippets or code from the internet, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. All right. Well, if information is taken into the CIA, it would then be important to delete any other versions of that,

right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. All right. You are aware of a general policy at the CIA that allows information to be brought into the CIA, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Mr. Schulte, it's not what this witness is here to testify about. Please limit yourself to the scope of his direct testimony. To the extent that you have argument to make, you'll certainly have an opportunity to make that at the close of the case.

BY MR. SCHULTE:

Q. After analyzing all the data you collected from my home computers, you didn't find Brutal Kangaroo, correct?

A. That's correct.

Q. No software from the CIA, right?

A. That's correct.

Q. No CIA backups, right?

A. That's correct.

Q. Slide 92, are you familiar with BKP extension?

A. Generally, an indication for backup or shorthand for backup.

Q. Hard drives and computers can fail, right?

A. Of course.

Q. As such, it's good practice to perform backups, right?

A. Of course.

Q. Here, five backup files are added to Eraser Portable, right?

A. Correct.

Q. The secure delete is not executed, right?

A. That's correct.

Q. It was canceled, right?

A. The program was closed before the execution was initiated, yes.

Q. So the five BKP files were never deleted, correct?

A. Not by Eraser Portable, no.

Q. So this seems to indicate that there was testing of Eraser Portable software, correct?

A. Correct.

Q. And there's also clear evidence that BKP files existed on my servers before the government claims I stole CIA backups, correct?

A. I'm not sure what evidence you're referring to.

Q. OK. During your forensic examination, you recovered one of the BKP files, correct?

A. Correct. Not one of the ones -- I don't believe one of the ones indicated here. The file recovers was data.bkp.

MR. SCHULTE: OK. I'm going to show just to the witness and the parties what's marked as defense exhibit 1406-1.

Q. Do you recognize this output here?

A. It appears to be metadata information about a file data.bkp.

Q. And through your forensic examination, you discovered a data.bkp file, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained. Asked and answered.

BY MR. SCHULTE:

Q. Did you examine the file that you recovered forensically?

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. Yes, I examined the data.bkp file.

MR. SCHULTE: I move to introduce 1406-1.

THE COURT: Is this reflected in another exhibit, Mr. Schulte, or no?

MR. SCHULTE: There is another exhibit, but we'd have to have a sidebar to discuss why it has to come in through this exhibit.

THE COURT: All right. Any objection, Mr. Lockard?

MR. LOCKARD: No objection to 1406-1.

THE COURT: Admitted.

(Defendant's Exhibit 1406-1 received in evidence)

BY MR. SCHULTE:

Q. So this is the file, correct?

A. I do not believe this is the copy of data.bkp that I analyzed, no.

Q. This is not data.bkp that you analyzed?

A. The data.bkp that I recovered was located within your home directory, the user profile Josh. This appears to be in a -- the root of a file system.

Q. OK. Well, it is a BKP file, correct?

A. It appears that way, yes.

Q. It's 21.4 gigabytes, right?

A. Approximately, yes.

Q. Well, do you recall ever reviewing this specific file?

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. I don't recall.

Q. But the file that you did review, it was not a CIA backup file, correct?

A. It was not.

Q. It was not a Stash backup, correct?

A. It was not.

MR. LOCKARD: Sidebar, your Honor?

THE COURT: OK. Ladies and gentlemen, you can stretch while we discuss at sidebar.

(Continued on next page)

(At sidebar)

THE COURT: Yes, Mr. Lockard.

MR. LOCKARD: So, your Honor, the file that Mr. Berger's being inquired about right now is an encrypted file recovered from the defendant's home computer that contained the child pornography. Right now, those counts have been severed, and we have not introduced any evidence relating to the child pornography charges. Mr. Schulte appears to be attempting to use that fact to suggest through Mr. Berger's testimony that it's an innocuous file when, in fact, the contents of that file support the government's theory that Mr. Schulte stored criminal files in data.bkp files. So we think that what Mr. Schulte is doing right now is opening the door to the fact that there is evidence of other crimes in the file that he's currently asking Mr. Berger about.

MR. SCHULTE: So, I just want to say first that we went through Judge Crotty on this, and these questions I'm asking are specific ones that were approved and were asked at the last trial. So I'm very specifically going through the previous trial and approved questions by Judge Crotty, where I'm asking if it's a CIA backup file and just establishing the fact that there's no classified information contained to that file.

That's the point of these questions. The whole point is there was data.bkp files that were deleted, so it's important to establish that these files are not CIA files, they're not Stash, they're not Confluence backups. That's the whole point of the cross.

MR. LOCKARD: I understand.

THE COURT: And that was permitted at the last trial.

MR. LOCKARD: I understand that is the point of the cross. I think that is an unfair argument to be making given the evidentiary posture we're in with respect to that file. And I also believe during the cross-examination of Mr. Berger at the last trial, the cross-examiner, when he realized what this file was, cut off any questioning about it.

THE COURT: OK. Well, I wasn't at the prior trial. No one asked me to adopt Judge Crotty's rulings on this particular issue, so as far as I'm concerned, it's fresh terrain.

That being said, why is it not proper for Mr. Schulte to just establish the point that there were BKP files on his computer prior to the date of the suspicious activity that the government suggests was his stealing of the Confluence backup and deletion of the Confluence backup? In other words, to the extent that the government has introduced evidence that those five BKP files that were not erased by Eraser Portable were wiped in some other fashion, isn't it fair game for him to establish that there were other BKP files that were on his computer that were unrelated to the CIA, and why do we need to even get into what they were?

MR. LOCKARD: The line of questioning, putting aside the content of data.bkp, there's nothing inappropriate about that line of questioning. I think where it's inappropriate is where Mr. Schulte is suggesting that it's an innocuous-type file.

MR. SCHULTE: The questions are just, is this a Stash backup? Is this a Confluence backup? Is there classified information? That's the line of questions.

MR. LOCKARD: That's already been covered.

MR. SCHULTE: I don't think we have.

THE COURT: I think he did just testify to that effect, so it's not clear to me what there is else to do with this, but I don't think that that alone opens the door to the effect that this may be contraband or evidence of a separate crime. So as long as we don't go any further than that --

MR. SCHULTE: Just those three questions.

THE COURT: All right. I think you've asked them. I'll check back, but if you have asked them, I think it's time to go to a different area of cross.

MR. SCHULTE: OK.

(Continued on next page)

(In open court)

THE COURT: All right. Thank you, ladies and gentlemen, for your patience.

Mr. Schulte, you may continue.

BY MR. SCHULTE:

Q. All right. Just to be clear, the BKP file does not contain any CIA documents, correct?

A. Correct.

Q. Moreover, this file was created at the very least by October 7, 2015, correct?

A. Correct. The file displayed here -- yes, that's correct, October 7, 2015.

Q. OK. Let's move on.

Back to your exhibit, 1704, slide No. 94. Many legitimate institutions use DBAN, correct?

A. I can't speak to that.

Q. Universities use DBAN, right?

A. I'm not aware of that.

Q. You're not aware that your university, NYU, uses DBAN?

A. They might use it. I am not aware of it.

(Defendant conferred with standby counsel)

Q. But DBAN itself is not nefarious software, correct?

A. Correct.

Q. Wiping is recommended activity in several situations, correct?

A. In some situations, yes.

Q. It's recommended when you're going to dispose of a hard drive, correct?

A. Correct.

Q. The IEEE computer society recommends securely wiping your drive, correct?

A. I would assume they do, yes.

Q. So we discussed the RAID and upgrade earlier, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. If you're going to upgrade your RAID, you would copy your data to an external drive, right?

A. Generally, yes.

Q. Then you delete the old RAID, right?

A. Correct.

Q. And you remove the old drives, right?

A. Correct.

Q. Then you install the new drives, correct?

A. Correct.

Q. And then you create the new RAID, correct?

A. Correct.

Q. And finally, copy of your data -- and finally, you would copy your data onto the new RAID, right?

A. Yes, that's one way of doing it.

Q. After this was completed, you would have at least two copies of your data, correct?

A. Correct.

Q. And most security protocols would then recommend securely deleting the old drives, right?

A. If you weren't maintaining them as some kind of backup copy and you were getting rid of them, then yes, you should -- you should be securely erasing it.

Q. Have you used DBAN on your home computer or devices to securely wipe data?

A. I have not.

Q. You've never used DBAN?

A. I have not. I've used it only in the context of this investigation, to virtualize it and just go through the menus and see what types of information and capabilities it describes.

Q. So what do you use to securely wipe your drives?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. OK. But DBAN would be consistent with this approach for upgrading a RAID, correct?

A. Not necessarily.

Q. It's not consistent?

A. The way DBAN works, it's a live operating system. It's intended that you want to wipe all the data on all the drives on the system, including the operating system drive. If you weren't wiping the operating system drive, you could use the utility while in your primary operating system to wipe any number of additional drives.

Q. OK. But if you -- in the process of upgrading the RAID, if you copy the data off the RAID, you would run DBAN then, right?

A. To wipe the drive -- if you're talking about wiping the drive that you backed up your RAID on, I wouldn't, because that's an external drive. I would still have the operating system of a computer to use another drive-wiping utility that is not in and of itself a live operating system. A live operating system would be used when you need to wipe the drives, including the drive that the operating system is located on, because you can't wipe the drive of an operating system while you're using that operating system.

Q. OK. Well, aside from what you would prefer to do, you can do it that way, correct?

A. You could boot up in DBAN and select an additional volume if it gives you the option.

Q. All I'm saying, once you copy the data off the old RAID, you can run DBAN just to wipe the old RAID, correct?

A. I don't recall. Based on the description of DBAN, it talks about how it will wipe the data of all the drives that it detects on the computer. So again, I would not risk doing that if I had the primary operating system drive that I did not intend on wiping.

Q. OK. Let me just be clear. You've, after you've removed all the data that you want and the old RAID is the only thing remaining, then you would use DBAN to wipe all those drives, correct?

MR. LOCKARD: Objection.

THE COURT: Overruled.

You may answer. I think you've answered, but just to be clear, you can answer.

A. So, I'm actually a little confused on what's being asked, what drives you're asking about being wiped. If you're talking about you've rebuilt your RAID and you have an external drive not connected to the computer that has a copy of that data, that's not something that I would use DBAN on.

Q. I think the point is -- let's just get past this, though. The point is you can use DBAN to wipe an old RAID, correct?

A. If by old RAID you mean an additional drive that's not connected to your computer, you could do it by connecting it to your computer, yes. I believe you were asking about wiping the drive you use as an intermediary backup while rebuilding your RAID.

Q. No. The question was about the old RAID.

A. The drives you removed from the old RAID array.

Q. Before you removed them from the old RAID array, after you've copied the data.

A. If you're talking about the drives from the old RAID array that are no longer in use and you wish to wipe them, again, you could use any number of wiping utilities. I would not expect DBAN to be the first choice, because you wouldn't need to. DBAN would be used when you want to wipe the entire system, including the drive of your operating system. If you had access to a drive and operating system, which you're using, there are any number of additional wiping utilities you could use without rebooting your computer into a live wiping utility.

Q. OK. But if you're upgrading, you have to do the reboot anyway, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Let's move on.

BY MR. SCHULTE:

Q. OK. Let's talk about Google searches here.

You know that there are searches for what you say, large data transfer confirmation, correct?

THE COURT: We're on slide 101 for the record.

A. There are searches about how long it takes to calculate an MD5 and an MD5 file. There are sites that are visited subsequent to the search that talks about verifying a one-terabyte file transferred correctly.

Q. OK. But that's a search result that's clicked on, right?

A. Correct.

Q. That's not what the search is, right?

A. That's correct.

Q. OK. So these searches are specifically for a file hashing speed, right?

A. A file hashing and file hashing speed, yes.

Q. And they're specifically related to MD5, right?

A. That's correct.

Q. MD5 is just the hashing algorithm, right?

A. Correct.

Q. And hashing and MD5 are not actually used in the transmission of data, correct?

A. Hashing MD5 is separate from the actual transmission of data, generally.

Q. Hashing can be used to verify the integrity of the transferred data, right?

A. Correct.

Q. But there are many uses for file hashing, correct?

A. Correct.

(Continued on next page)

Q. These are all examples of using hashing, right?

A. Correct.

Q. And with respect to data integrity, if you were copying data from an old system before an upgrade you would run an ND-5 to ensure data integrity, correct?

A. It's possible, yes.

Q. And I consistently conducted similar searches for hashing, correct?

A. Could you describe what you mean by consistently?

Q. Yes. I'm going to show, just to the parties, Defendant's Exhibit 302-5.

MR. LOCKARD: No objection.

THE COURT: Are you offering it?

MR. SCHULTE: Yes.

THE COURT: OK. Admitted.

(Defendant's Exhibit 302-5 received in evidence)

BY MR. SCHULTE:

Q. May 3rd there is search for Linux copy large file has, correct?

A. Correct.

Q. May 10th there is a search for fast hashing algorithm, correct?

A. Correct?

Q. And a month later, in June, there is a search and Wikipedia visit for specific types of hashing, correct?

A. Yes.

Q. And then a few days later, June 6, there is a search for a comparison of F&V and CRC 32, right?

A. It appears that way, yes.

Q. And, specifically, the visited page references hashing algorithm by uniqueness and speed, correct?

A. Correct.

Q. And there are even hashing algorithm searches before May, correct? Not on this slide, I will take this down. 302-6, I will show the witness. Do you recognize these kinds of output here?

A. Again, it appears to be search results.

MR. SCHULTE: I move to admit this one, too, 302-6.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 302-6 received in evidence)

BY MR. SCHULTE:

Q. April 4 there is a search for sha1sum, correct?

A. Correct.

Q. And Sha1 is just another hashing algorithm, right?

A. Correct.

Q. April 24th there is a search for Sha1 sum power sha, right?

A. Correct.

Q. And there is search for file check sum integrity verifier, correct?

A. Correct.

Q. And then a visit it a Microsoft page to download that, right?

A. It is not clear from the Microsoft URL what is at that page.

Q. It is some kind of downloader. There is a download in the link, right?

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. It appears to link something from Microsoft but it is not clear from the URL again what is being downloaded.

Q. Would you agree that data integrity is a crucial component of any storage server?

A. Yes.

Q. Do you also agree that hashing, and particularly conducting speedy hashes, is critical in my job of writing malware to copy data?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Q. I think we saw earlier an exhibit about developing software that copies data from thumb drives, correct?

A. Sounds familiar.

Q. I think you just testified about it earlier on the cross but, again, hashing would be important for that kind of software, right?

A. Again, if there was a specific need to implement hashing that would be important.

Q. Well, for copying data it is important, right?

A. If you were concerned about the integrity of copying the data, yes.

Q. And also to ensure that you are not re-collecting the same data, right?

MR. LOCKARD: Objection.

THE COURT: Is there an objection?

MR. LOCKARD: There is an objection.

THE COURT: Overruled.

A. That could be another reason why you would use hashing, yes.

Q. There is nothing unique about the searches that you picked out, correct?

A. The searches that were picked out indicated searches for specific items. There are other entries for similar searches, yes.

Q. Next is going to be wiping on slide 102. You identified Google searches about wiping hard drives, correct?

A. Correct.

Q. Searches were conducted May 1, 2016; right?

A. These appear to be from April 30th and the two at the bottom from May 4, not May 1.

Q. OK. The searches on May 4th for: Can you use DBAN on SSD, right?

A. Yes.

Q. And I think on slide 96 you showed DBAN ISO was downloaded at 11:28 a.m.?

A. Correct.

Q. And like, as you said, solid state drives are different from typical platter mechanical drives, correct?

A. Correct.

Q. So there are different ways you would be wiping solid state drives, correct?

A. That's correct.

Q. And like you said I think on direct, DBAN is not ideal for solid state drives, correct?

A. That's correct.

Q. And I think you also said you would want to download the wiping software specifically from the manufacturer, right?

A. Generally, yes.

Q. So slide 103, I am going to talk about the hard drives here. I will pull up what's in evidence as Government Exhibit 1636.

And these are the devices recovered from my apartment, correct?

A. I believe so, yes.

Q. There were many loose hard drives discovered, correct?

A. I believe so, yes.

Q. And by loose hard drives I simply mean that these drives are not connected to any computer, right?

A. Correct.

Q. And all of these drives are zeroed, correct?

A. The ones indicated I believe on the slide in the presentation were zeroed, yes.

Q. And it is good security practice to wipe the drives when you are no longer using them, correct?

A. If you are going to be disposing of them, yes.

Q. Well, you can't really say whether these are newly purchased drives or wiped drives, correct?

A. Generally newly purchased drives would have something on them, at minimum some kind of file system. Many times they also come with some kind of utility software from the manufacturer.

Q. Well, not if they're purchased through a third-party, right?

A. It's possible that the drives come without anything on them but again, generally there is usually some kind of file system on them.

Q. I'm talking about purchasing them from another individual.

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. So if you are buying them from another person it would depend on if that person wipes them or not.

Q. And so you cannot say when these drives were zeroed, correct?

A. That's correct.

Q. You can't say how old the drives are, right?

A. That's correct.

Q. Moving on to slide 104, you testified on direct that I repeatedly unlocked my home computer, correct?

A. Correct.

Q. The logs you referenced were not logs from my home computer, correct?

A. They were from the virtual machine which was on your home computer.

Q. But there is no -- absolutely no forensic evidence to support your theory that the virtual machine was ever on my home computer in April of 2016, correct?

A. It was found on your home machine.

Q. It was found on my home machine that had been installed on May 5, right?

A. Your home machine was re-formatted on May 5, correct.

Q. Newly installed or re-formatted, you don't know what happened before that, right?

A. We have some idea, yes.

Q. You don't know where this virtual machine was located before May 5, right?

A. Not with a hundred percent certainty, no.

Q. You are not speculating because it was copied to the home computer on May 5 that it existed before then, correct?

A. I wouldn't characterize it as speculation.

Q. No?

A. No.

Q. There is forensic evidence to back it up?

A. There is evidence that it was used by you prior to that date, in fact several days prior to May 5. That would indicate it was on a computer system that you had accessed it.

Q. But you don't know who was actually using it, the VM; right?

A. Who was using the virtual machine, it is indicative by the layers of security mechanisms that were on there and how they were unlocked with passwords known to you that indicated that you were most likely using that machine.

Q. You don't know if those were shared passwords, right?

A. I don't know that, no.

Q. You don't know if this VM was stored on a NAS or a different computer than my home computer, right?

A. I can't say that for sure, no.

Q. In fact, the VM was last used on May 1, 2016, right?

A. I believe so.

Q. It was then copied to the new RAID system on May 5, right?

A. I believe so.

Q. After that copy the VM was never used again, right?

A. Sounds about right.

Q. In fact, I did not download VirtualBox until August 4, 2016; correct?

A. I don't recall.

Q. I am going to show what is marked as Defendant's Exhibit 1401 -- or 1402-1, for just the witness and the parties. You recognize this kind of output, right?

A. It appears to be metadata information from some type of -- possibly -- forensic program.

Q. And these types of tools would be used to collect forensic artifacts from hard drives, correct?

A. Forensic programs would be, yes.

MR. SCHULTE: I move to introduce Defendant's Exhibit 1401.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 1401 received in evidence)

BY MR. SCHULTE:

Q. This shows VirtualBox downloaded on August 4, 2016; correct?

A. So I can't confirm that from this particular artifact.

Q. Why is that?

A. It's not an artifact that pertains to the file system information. Based on what I am looking at here, it talks about a key last updated, date and time. The August 4th date that you mentioned is actually found in a registry key that is located down at the bottom under current control set 1, specifically the app compatibility cache, which is a mechanism within Windows utilized to find resources that programs need to run but it does not indicate when the actual file was created in this case on the D drive.

Q. VirtualBox is a software used to create or use this type of VM, correct?

A. Yes. VirtualBox can be used to create virtual machines and run them.

Q. I am just talking about specifically the VM that was located on the home computer.

A. Yes. I believe it is a VirtualBox formatted VM, yes.

Q. I will take it down for the jury and show 1402-1. Do you recognize this type of output, too?

A. Yes. It appears to be, again, forensic or metadata details from some forensic program.

MR. SCHULTE: I move to introduce this.

THE COURT: No objection. Admitted.

(Defendant's Exhibit 1402-1 received in evidence)

BY MR. SCHULTE:

Q. And this shows download of a VirtualBox version 5.1.14, correct?

A. It appears so, yes.

Q. January 23rd, 2017; right?

A. It appears that way, yes.

Q. I'm going to show what's marked as 1402-3. Do you recognize this output as well?

A. Yes. Again, it appears to be forensic artifacts from a forensic analysis program.

MR. SCHULTE: I move to introduce 1402-3.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 1402-3 received in evidence)

BY MR. SCHULTE:

Q. So this is showing the installation of VirtualBox 5.1.14, correct?

A. It could be installation or could be modification of the program. Specifically this artifact shows, again, a last update of a registry key, specifically within Windows, the current version uninstall. This would be where a program being installed places reference material so that the program can be easily uninstalled. It is possible it was created during installation of the program or possibly an update of the program when you run the installer and click modify or change the details of the installation.

Q. But this is January 2017, right?

A. Yes, it is.

Q. But after VirtualBox is installed the virtual machine found on my desktop is still never used, correct?

A. I don't recall the exact last date that it was used or modified. I know it -- I believe it had sat unused for some time before it was obtained in March of 2017.

Q. I am going to show what's marked as Defendant's Exhibit

1404 just to the parties. Do you recognize this kind of data?

A. Yes. Again, it seems to be forensic artifacts from some forensic analysis program.

MR. SCHULTE: I move to introduce this as well.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 1404 received in evidence)

BY MR. SCHULTE:

Q. So this shows last modified of May 1st, 2016; correct?

A. Correct.

Q. And the May 6, 2016 fields are an artifact of copying it, correct?

A. Usually, yes.

Q. To move on for a moment to what is marked as Defendant's Exhibit 302-3, showing this just to the witness and the parties? Do you recognize this type of output?

A. It appears to be similar to the Google search results that I have seen.

MR. SCHULTE: I move to introduce this as a sub-exhibit through government's Google searches.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 302-3 received in evidence)

BY MR. SCHULTE:

Q. So 302-3, and it shows searches for League of Legends config data, correct? At the bottom?

A. It appears so, yes.

Q. Do you know what time this is searched for?

A. The last entry there looks like it was May 1st at 4:23 in the morning UTC, so that would be 12:23, or 23 minutes after midnight, local time.

Q. And League of Legends is a video game, correct?

A. I believe so, yes.

Q. From your forensic examination were you able to determine that I was -- that I often stayed up very late playing League of Legends?

A. Somewhere along the investigation I remember hearing that you did play League of Legends. I did not conduct any particular forensic analysis relating to your game-playing activities.

Q. But that would have been important data for your analysis, correct?

A. I'm not sure what you mean by that.

Q. Well, as establishing habits or normal routine it's relevant, right?

A. Not necessarily relevant to just looking for forensic artifacts, no.

Q. I mean, if somebody is staying up until 4:00 a.m. playing video games that is relevant to the investigation, right?

A. It might be relevant to the overall investigation, sure.

Q. And, in fact, during this time on May 1st there were several League of Legends files that were modified, correct?

A. I can't speak to that.

Q. OK. I'm going to show just the parties what is marked as Defendant's Exhibit 1407-1. Do you recognize this type of output?

A. Appears to be a listing of files and metadata information about those files.

Q. And through forensic investigations you would pull directly listings of files, correct?

A. I might look at file listing information within certain directories, yes.

MR. SCHULTE: I move to introduce 1407-1.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 1407-1 received in evidence)

BY MR. SCHULTE:

Q. So the files lists here have date, time stamps, and their names; correct?

A. It appears so, yes.

Q. 2016-04-30, correct?

A. Yes, they all begin with 2016-04-30.

Q. That's April 30th, 2016, right?

A. Yes.

Q. 20:41:31 was the time, right?

A. It appears that way, yes.

Q. That's 8:40 p.m., correct?

A. If that is in local time, so yes, 20:41 would be 8:41 p.m.

Q. Finally, I want to show the other, something that's marked as 1407-2. This is the same kind of output, correct?

A. It looks similar. There appears to be a listing of files and modified time stamps.

MR. SCHULTE: I move to introduce 1407-2.

MR. LOCKARD: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 1407-2 received in evidence)

BY MR. SCHULTE:

Q. From these file paths this is League of Legends, correct?

A. It would appear that way, yes.

Q. And the date modified is showing midnight, May 1, 2016; right?

A. Midnight UTC, yes, so subtract four hours so that first one at midnight and 41 minutes UTC would be about 8:41 p.m. on the evening of April 30th, I believe.

Q. And then the last modification times are showing 3:30 a.m., correct?

A. Yes. So the last few lines there that shows 3:27 a.m. UTC would be translated to 11:27 p.m. the evening of April 30th, 2016.

Q. So even assuming that the virtual machine existed on my home computer on April 30th, the forensic examination suggests that this system was used to download data as opposed to send data, correct?

MR. LOCKARD: Objection.

THE COURT: Overruled.

A. I'm not sure where you are getting that indication from. It appears the computer was used for many different purposes including playing video games.

Q. No. I'm sorry. I am talking about your forensic examination of the virtual machine.

A. Can you repeat the question?

Q. Yes. The forensic examination of that virtual machine strongly suggests it was used to download data as opposed to transmit data, correct?

A. There was more evidence within the virtual machine of data being downloaded than uploaded, correct.

Q. You did not find forensic evidence that suggests data was transmitted or -- I'm sorry. Let me rephrase.

You did not find forensic evidence that suggests large data was transmitted from the VM, correct?

A. Correct.

Q. You did not find any evidence that CIA data was stored or transmitted from the VM, correct?

A. I did not find any forensic artifacts like that, no.

Q. You did not find any evidence that any CIA backups were stored or transmitted from that virtual machine, right?

A. Correct.

Q. In fact, you did not find any browser history or forensic artifacts that showed visits to WikiLeaks, correct?

A. I don't believe so, no.

Q. So there is no evidence anything was ever transmitted to WikiLeaks, correct?

A. Incorrect.

Q. Incorrect.

You found evidence that information was transmitted to WikiLeaks from the VM?

A. I believe your previous question didn't specify VM and only asked about evidence that data was transmitted to WikiLeaks. The evidence that data transmitted to WikiLeaks is that the data showed up on WikiLeaks.

Q. OK. So that's evidence that WikiLeaks received the data, correct?

A. Correct.

Q. That's not evidence that I transmitted anything to WikiLeaks, correct?

A. It is evidence the data was transmitted to WikiLeaks.

Q. The question was did you find any evidence from the forensic examination that anything was transmitted to WikiLeaks.

A. Forensic artifacts on virtual machine, no.

Q. Any forensic artifacts?

A. The entirety of my analysis was forensic artifacts, so yes.

Q. Yes what?

A. Yes, there was evidence that data was transmitted to WikiLeaks, as I mentioned.

Q. What are those forensic evidence?

A. That would include the timing analysis I conducted, as well as the analysis and testimony of Mr. Leedom. That's the evidence that data was transmitted to WikiLeaks, specifically the March 3rd backups.

Q. I'm asking about forensic evidence, specifically from my home.

A. Again, if we are talking about forensic artifacts within the virtual machine, no.

Q. No, not just the virtual machine, my entire home. All the electronic devices you analyzed from my home, is there any forensic evidence that suggests any data was transmitted to WikiLeaks from any of the frenzy artifacts.

A. No.

Q. OK. So let's end by talking about the alleged transfer of data to WikiLeaks. You were present during Mr. Leedom's testimony, correct?

A. Yes.

Q. Mr. Leedom testified that his forensic findings were that the March 3rd, 2016 backup file was accessed on April 20th, 2016; correct?

A. Correct.

Q. Mr. Leedom found no forensic evidence that the March 3rd, 2016 Confluence backup was copied but he speculated that I copied it on April 20th, 2016; correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Q. Well, based on Mr. Leedom's theory, you were tasked with essentially working backwards from the April 20th, 2016 date, correct?

A. That's incorrect.

Q. You were not told data was stolen April 20th so look for data transfers after this date?

A. That is not correct.

Q. What were you told?

A. When I was tasked for performing the timing analysis I was tasked with simply identifying the data from which the data on WikiLeaks was disclosed came from. At the time that I performed that analysis it had not yet been discovered about the modified access time on the March 3rd backups. That was discovered several months later, I believe.

Q. OK. I'm not talking about the timing analysis, I am just focused on your forensic examinations of the home electronics.

When you were examining the home electronics were you told to search for data transfers after April 20th?

A. I was not. When I first started analyzing the evidence recovered from your apartment the activity that occurred on April 20th had not been detected yet.

Q. But at some point you were tasked with collecting data to support the conclusion that the backups were transmitted to WikiLeaks after April 20th, right?

A. I don't believe so, no.

Q. Well, all forensic artifacts from my home computer prior to the latest installation on May 5 were lost, correct?

A. If you are referring to activity on files that were modified prior to that date then, no, there is evidence of files being modified and being moved back to the system after you re-formatted them and those files have last modified dates prior to the reformatting.

Q. OK, but specifically about system logs or jump lists or any information that Windows would keep track of, that information was no longer available, correct?

A. No, that would not be preserved after the re-format.

Q. So an examination of the system after May 5 shows that there were no CIA hard drives connected, correct?

MR. LOCKARD: Objection.

THE COURT: Do you want to reformulate the question, Mr. Schulte?

MR. SCHULTE: Yes.

Q. So what I am trying to get at here, your window -- based on the forensics that you analyzed, your window was between April 20th and May 5th because the home computer was installed on May 5th, right?

A. I'm not sure what you mean by window. What -- can you clarify what time -- what window you are referring to?

Q. A window of transmission of data to WikiLeaks.

A. Yes.

Q. So if there is forensic evidence to show that it was impossible to transmit the Stash and Confluence backups between this window, the government's theory is forensically and technically impossible, correct?

A. I don't know what evidence you are referring to.

Q. I'm about to get to it, but I'm asking if that's established then the government's case is not possible, right?

A. I can't speak to the entirety of the government's case. I can only speak to what I have testified about.

Q. OK. Well, the minimum size of data sent to WikiLeaks, you testified on direct, was about 200 gigabytes, right?

A. Somewhere around there, yes.

Q. So 200 gigabytes had to be transferred between that time frame April 20th to May 5, correct?

A. It didn't necessarily have to have been completed by May 5 but it makes sense that it would have been completed by May 5, yes.

Q. Well, if it wasn't completed by May 5 then there would be forensic artifacts or evidence of that that you would have discovered after May 5, correct?

A. Only if there was continued transmission on that particular system, yes.

Q. So is your theory that the data was transmitted using the virtual machine between midnight and 3:00 a.m. on May 1st?

A. I'm not sure if the virtual machine was used to transmit the data, no.

Q. So you don't have a time frame about when the data was transmitted; is that right?

A. My opinion is it was transmitted during that time period prior to reformatting because of all the other evidence, including the drive wiping and reformatting, yes.

Q. I'm sorry. So what time period is that, just to be clear?

A. Between April 20th and May 5th.

Q. OK. But you are aware that using TOR is a substantial bottleneck, correct?

A. Yes, it does reduce your connection speed.

Q. The highest average TOR bandwidth is about five megabytes per second, correct?

A. I don't know the exact specifics of the bandwidth.

Q. All right. I am going to show what's marked Defendant's Exhibit 1411-1.

Are you aware that TOR monitors, keeps track of bandwidth?

A. I don't know exactly what specific metrics they monitor.

Q. You know generally though, right?

A. The artifact that I am very familiar with is that they keep track of a list of what are referred to as TOR exit notes that is useful in FBI investigations if an investigation resolves to an IP address and we want to determine if at a particular date and time that IP address was actually running as a TOR exit mode. Other types of metrics and statistics they keep track of. I can't speak to any real familiarity with those.

Q. I mean, through your investigation you investigated TOR, right?

A. I was familiar with TOR prior to this investigation. I believe I might have looked up a few things over the course of this investigation.

Q. Well, analyzing the feasibility of data transfer would have been very important to your investigation, correct?

A. Could you clarify what you mean by feasibility of the data transfer?

Q. Yes. If you selected a time frame that you believe the data was transferred but it wasn't feasible to transfer that data in that amount of time, that would have been important, right?

A. Yes.

Q. OK. You made slides about TOR in your presentation, right?

A. Correct.

Q. So the amount of bandwidth that can be sent across TOR is a very important factor to your investigation, correct?

A. If the data was definitely transmitted over TOR, yes.

Q. Is your theory -- isn't your theory that this data was transmitted over TOR?

A. My theory is that the data was transmitted to WikiLeaks.

Q. So do you believe TOR was involved in that transfer? Or not.

A. I believe TOR was involved possibly at the beginning, however one of the things WikiLeaks indicates on their site -- I believe it was in one of the slides in my presentation -- was that where you say how you connect to them and use TOR and go to their .onion URL they have a specific note and say please contact us if you have very large files you want to send us. It is reasonable to infer to that if you reached out to them and someone said I have very large files that I wish to transfer, they might provide an alternative upload connection that did not involve TOR because of the reduced speeds of TOR.

Q. Well, the whole point of using TOR is to be secure and private about the transfer, right?

A. That's one use of TOR, yes.

Q. So it wouldn't really make sense to tell someone to use something else when the whole point is to use TOR to transmit it securely, right?

A. There are other methods of transmitting data securely.

Q. Your slide presentation does not make any indication of that though, does it?

A. Again, I believe it's in one of these screenshots that I took from the WikiLeaks archival copy from the Wayback Machine. I believe it describes that there.

Q. OK. You would agree, though, that the throughput of TOR is a relevant factor to the investigation though, right?

A. Again, it could be.

Q. OK.

MR. SCHULTE: I move to introduce Defendant's Exhibit 1411-1.

MR. LOCKARD: Objection.

THE COURT: Sustained.

Q. Showing just to the witness and parties exhibit marked Defendant's Exhibit 1411-2.

Through your investigation into TOR, were you able to determine the statistics that they provide?

A. Again, my part of the investigation did not really focus in on TOR other than possibly researching one or two aspects and I don't recall ever looking into statistics other than, as I mentioned, just in general FBI investigations when we consult the list of TOR exit modes.

Q. All right. I will take that down.

You have heard of Internet Service Providers, correct?

A. Yes.

Q. What are ISPs?

A. From a residential perspective they provide Internet connections to people's residences. They can also provide commercial Internet connections to places of business.

Q. ISPs keep data of their customers, correct?

A. To some extent, yes.

Q. You have heard of NetFlow logs, right?

A. I have.

Q. Mr. Leedom testified about NetFlow logs, right?

A. I believe he testified that there were no NetFlow logs when he first arrived for the investigation.

Q. Correct.

But NetFlow logs show the amount of data available, both transmitted and received; correct?

A. Generally speaking, yes.

Q. And Verizon was my ISP in 2016, correct?

A. That sounds familiar, yes.

Q. And Verizon kept NetFlow logs during that time, correct?

A. I'm not aware of that, no.

Q. You are not aware of whether or not Verizon kept NetFlow logs?

MR. LOCKARD: Objection.

THE COURT: Sustained. Asked and answered.

BY MR. SCHULTE:

Q. OK. Well, NetFlow logs would establish definitively whether or not data was transmitted or received during this time period, correct?

A. If, depending on the records, they would establish what data was transferred or received over the connection from Verizon, yes.

Q. Verizon was my ISP, right?

A. Again, I believe so.

Q. So Verizon would actually have the logs of what data I sent between April 20th and May 5th, 2016, right?

A. If they retained those records, yes, they would have the logs of what data was sent or received over your connection with them.

Q. I want to show to the parties what is marked as Defendant's Exhibit 208. It is a very large file so I think it's having some problems.

Pursuant to the stipulation 3006, the Verizon NetFlow logs are provided as Defendant's Exhibit 208.

MR. LOCKARD: Objection to the characterization but no objection to the document.

THE COURT: Well, I don't know if we can display it but Defendant's Exhibit 208 is admitted, without objection.

(Defendant's Exhibit 208 received in evidence)

BY MR. SCHULTE:

Q. It is taking a minute to display. There are sub-exhibits 208-1 through 8. This might be easier if the government has reviewed those and agrees to admit those now or we can just go through the big data.

THE COURT: Is there any disagreement that they're just extractions from 208?

MR. LOCKARD: I am not aware, but if we can hold them up we can take a look at them one by one.

THE COURT: Can you pull them up one by one, please?

MR. SCHULTE: Do you want to pull up the sub-exhibits first or the big one first?

THE COURT: Since the big one is not coming up let's do the sub first and then hopefully that will take care of it.

MR. LOCKARD: Your Honor, I think we do have an issue with this.

THE COURT: This being which?

MR. LOCKARD: I don't think we were previously provided 208-1, etc.

MR. SCHULTE: Yes, it was --

THE COURT: So let's just stick with 208 which is in evidence. Mr. Schulte, if you can't pull it up, move on to the next line of questioning.

MR. SCHULTE: OK.

THE COURT: Do you have another line of questioning? Maybe standby counsel can try to pull this up while you move on.

MR. SCHULTE: This is the final exhibits, 208-1 through 8 -- there it goes. This is the final line of questioning.

BY MR. SCHULTE:

Q. So 208 is in evidence so I will publish that. And the government does not agree to --

THE COURT: Mr. Schulte, ask your next question, please.

MR. SCHULTE: OK.

BY MR. SCHULTE:

Q. So these show the NetFlow logs from Verizon, correct?

A. It looks like it is some type of NetFlow data. I can't speak to where it's from.

THE COURT: Just to help the jury here, just a reminder that the stipulation that was admitted as Government Exhibit 3006, which Mr. Schulte read earlier, did verify that Defendant's Exhibit 208 -- this document -- is a true and correct copy of records from Verizon and doesn't characterize what they are but it is a Verizon record.

Go ahead.

BY MR. SCHULTE:

Q. So do you recall Mr. Leedom's testimony, his final thing in his slide that I locked up the vault at 7:07 p.m. on April 20th?

A. Yes. That sounds familiar.

Q. 1907.

So if we use this as a starting point, you would agree that from a conservative standpoint this is the earliest that the data could be transferred to WikiLeaks, correct?

A. Through Verizon, yes.

THE COURT: Can you just make a record of what row you are on or some other record, please?

MR. SCHULTE: So it is row 1,613,641 and I am just going to mark that and then we are going to clear out the beginning ones.

MR. LOCKARD: Objection.

THE COURT: Sustained. Let's leave the exhibit as it is, please.

MR. SCHULTE: This is to establish the sub-exhibits. If the government doesn't acknowledge them then --

THE COURT: Tell you what. I just think it is better that we have a single exhibit and that we are not changing it, so let's leave it as is but you have made a record of what that row is. Proceed.

MR. SCHULTE: I think the problem is going to be that this file is too big to be opened in Excel so we have to cut it down in order to open it.

THE COURT: That really should have been done earlier. I will allow you to delete the prior lines and then we will re-save it as 208, let's say A, and essentially treat it as a modified version.

MR. SCHULTE: OK.

THE COURT: So just to be clear, am I correct you have deleted all the rows before that 1,613,000 row that corresponds to April 20th at 7:07? Is that correct?

MR. SCHULTE: That's correct.

THE COURT: OK.

BY MR. SCHULTE:

Q. So like you said, from the most conservative approach, 7:07 p.m. on April 20th is when the vault is locked up, correct?

A. I believe so.

Q. And so then the end date for your calculation would be May 6th, 2016, correct?

A. I believe so, yes.

Q. And that time on May 6 would be -- let's just pull up -- I will pull up your slide and establish the computer is showing a May 5, 2016 re-format, correct?

A. Correct.

Q. So again, a conservative range would be May 6, 2016 because that would encompass all of the data, right?

A. For the data to be transmitted using that computer, yes.

Q. You would agree that this line, 356061, would represent that; correct?

A. It seems so, yes.

MR. LOCKARD: Your Honor, we object to any further questions about this exhibit.

THE COURT: Overruled.

BY MR. SCHULTE:

Q. So this data after it, we can remove this data too, right, starting at 356062?

A. You can remove whatever you want from it.

Q. What I am trying to do is narrow down your range so we can look at it properly.

THE COURT: He testified that assuming this machine was used it had to be before that date, so go ahead and delete it if you want to delete it and ask your next question.

MR. SCHULTE: All right.

So according to the NetFlow logs -- once we are able to pull that up in Excel we can -- there is two sets of data that the NetFlow will provide us, correct?

MR. LOCKARD: Object to the form.

MR. SCHULTE: Let me rephrase.

Q. The NetFlow logs show data that you received and data that you transmitted, correct?

A. I believe so, yes.

Q. So the extra data after this has been removed as to save this as 208-B?

THE COURT: I don't think we need to complicate things further. Isn't still 208-A just an excerpt version of 208?

(Continued on next page)

MR. SCHULTE: OK. Yes. That's fine.

THE COURT: OK. I'll deem that admitted as well.

MR. SCHULTE: OK. So, let me take this down.

Now I'm going to show the data in Excel. Can the parties see the exhibit?

THE COURT: Mr. Schulte.

MR. SCHULTE: Yes. The computer just died.

THE COURT: Maybe we should proceed with redirect, and then I'll give you permission to return to this on recross. In the meantime, you can try and fix the technical issues.

MR. SCHULTE: Yes. It's -- no. It's back.

THE COURT: OK.

MR. SCHULTE: It's back, so I don't know what we should do.

Q. So this data represents the data transferred, correct?

MR. LOCKARD: Objection. Foundation.

THE COURT: I think that is a foundation question.

You can answer, if you know.

A. In my understanding, it would appear to represent, at minimum, a subset of data transferred over the Verizon connection during that time period. Having never actually been presented this or been able to conduct my own analysis on it, I don't know really what I can answer about it.

Q. I mean we just opened it up and cut down to the relevant data, right?

A. You reduced it down to the period from April 20 through May 6, I believe, yes.

Q. OK. But this data is showing data that was both transmitted and received, correct?

MR. LOCKARD: Objection. Foundation.

THE COURT: Again, the witness can answer yes or no, or you don't know.

A. It does not appear to indicate that. There's a -- does not appear to indicate data both sent and received.

Q. You see a consistent IP address through all the source and destination address, correct?

A. I see IP addresses under the source address and destination address columns, yes.

Q. I'm saying this specific IP address, 71.178.235.3, you see that through all source and destination, all through it, right?

MR. LOCKARD: Objection. It's a 350,000-line spreadsheet.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. When Verizon, Verizon -- this is an exhibit provided by Verizon, as we've established, and it shows data from a specific IP address, correct?

A. It shows data that would be on the connection. However, you asked if it shows data sent and received, and from what I can see here, data is measured in the volume of data which would be normally indicated in bytes or some variation of. There's a singular column that says bytes. Normally, with a session of data, you are -- have a session that's open between two hosts and there's data sent, there's data received. In this case, just the total volume transferred between those two addresses, I don't know if that's an indication of from source to destination or if it's the total amount of data that was exchanged between both of those over that particular connection.

Q. OK. But acknowledging that this record is provided by Verizon, it accounts for both data transmitted and received, right?

MR. LOCKARD: Objection.

THE COURT: Mr. Berger, have you seen these Verizon records before?

THE WITNESS: I have not.

THE COURT: Are you familiar with what is included or not included in Verizon records?

THE WITNESS: I am not. I'm familiar with the general concept of NetFlow data, which can vary depending on the provider or device manufacturer.

THE COURT: Sustained.

And we're going to be done with this line of questioning. If that's the last one, then we'll proceed with redirect. Anything else, Mr. Schulte?

MR. SCHULTE: I just --

THE COURT: Mr. Schulte, anything else?

MR. SCHULTE: Yes.

Q. I just want to establish that through your understanding of NetFlow logs in general, it's going to list all the data. NetFlow log lists all the data, correct?

A. NetFlow logs generally list metadata. However, NetFlow logs can be -- the data that's within a NetFlow can be determined by who created it, specifically if there were a certain type of protocol included or excluded or certain types of activity. Without knowing exactly how they generated their NetFlow or what the parameters were, I can't speak to that.

Q. Well, without any specifics about what the provider, how the provider provides the data, you understand from NetFlow logs the type of data NetFlow logs represent, right?

A. Yes, NetFlow is the metadata about network connections.

Q. OK. So based on your knowledge of NetFlow logs, if we sum up all the bytes here, that would tell us the total amount of data transmitted and received, correct?

MR. LOCKARD: Objection.

THE COURT: Sustained.

Mr. Schulte, we're well beyond the scope here. All right? If you have one more question, I'll allow you to ask it. Otherwise, we'll proceed with redirect.

(Defendant conferred with standby counsel)

MR. SCHULTE: I just note for the Court this was one of the witnesses I wanted to go beyond the cross. If not, I can re-call him in the defense case.

THE COURT: All right. Well, we'll discuss that and proceed with redirect now.

MR. LOCKARD: Your Honor, if I may, do we expect to end at 2:45?

THE COURT: Well, I very much hope so. I'd like to stick to the schedule. How long do you expect the redirect to be?

MR. LOCKARD: I'm just looking for what time we expect to end. That's all.

THE COURT: 2:45.

MR. LOCKARD: Thank you.

REDIRECT EXAMINATION

BY MR. LOCKARD:

Q. Good afternoon, Mr. Berger.

A. Good afternoon.

Q. During your cross-examination, you were asked a number of questions about what forensic artifacts you did and did not find on the defendant's home computing computer equipment. Do you recall that?

A. Yes.

Q. Did you find forensic artifacts of CIA data on the defendant's home computers?

A. Not -- nothing other than the one reference to Brutal Kangaroo.

Q. OK. We'll come back to that.

Did you find forensic artifacts of the defendant's communications with WikiLeaks on his home computers?

A. I did not.

Q. Did you find forensic artifacts of the defendant's transmission of data to WikiLeaks on the defendant's home computers?

A. I did not.

Q. What types of forensic artifacts would be relevant to those kinds of issues?

A. What types of artifacts would indicate that type of activity? Is that what you're asking?

MR. SCHULTE: Objection to form.

MR. LOCKARD: Let me rephrase.

If we could pull up Government Exhibit 1704, and if we could go to page 72.

Q. Did you find forensic artifacts of the defendant's downloading of the Tails live operating system?

A. I did.

Q. What is the effect of using the Tails live operating system?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. It prevents anything from being retained as forensic artifacts on your hard drive.

MR. LOCKARD: If we can go to page 64, please.

Q. And is that, in fact, how Tails describes its own system?

A. Yes.

MR. SCHULTE: Objection.

THE COURT: Sustained as to form.

BY MR. LOCKARD:

Q. How does Tails describe the effect of using Tails on leaving traces on the computer you're using?

A. It specifically lists that it leaves no trace on the computers you are using unless you ask it implicitly.

Q. Can Tails be used on a desktop?

A. Yes.

Q. Can Tails be used on a virtual machine?

A. I believe so.

Q. Would what effect would there be of using Tails on a virtual machine?

A. If you use Tails as a virtual machine, the operating system would boot again completely in memory. There would be some artifacts left on the host computer, the desktop, that you did, in fact, create a virtual machine from the Tails ISO files downloaded.

Q. What would be the effect of using Tails on the desktop itself?

A. There would be no artifacts left if you booted up off of Tails on the desktop.

MR. LOCKARD: If we can go to page 62 of Government Exhibit 1704.

Q. What does WikiLeaks recommend about Tails?

MR. SCHULTE: Objection.

THE COURT: All right. It speaks for itself.

Next question.

BY MR. LOCKARD:

Q. You were asked some questions about TOR and whether there are legitimate uses of TOR and legitimate users of TOR?

A. Correct.

MR. LOCKARD: If we could turn to page 60.

Q. Is WikiLeaks one of those advocates of TOR?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. Yes, WikiLeaks advises that in order to use their public submission system, that you need to download TOR and connect to their TOR hidden service URL.

Q. What is the effect of using a TOR browser of an investigator's ability to recover forensic artifacts of activity using TOR?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. Makes it very difficult.

Q. You were also asked some questions about the defendant's Google search history. Do you recall those questions?

A. Yes.

Q. And specifically, questions about whether the defendant had searched for or visited the WikiLeaks site using his Google account?

A. Yes.

Q. What, if any, forensic artifacts would be left using TOR to visit the WikiLeaks site?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. The TOR browser is designed to leave as few forensic artifacts as possible.

THE COURT: Just to flesh that out, if someone used TOR to access WikiLeaks, would there be forensic artifacts of that, or no?

THE WITNESS: It's possible, but most likely no.

MR. LOCKARD: If we could turn to page 56 of Government Exhibit 1704.

Q. So here, on this page from WikiLeaks, there's a large URL there in the center. What is the significance of the dot-onion URL?

A. Again, the dot-onion URL indicates a TOR hidden service; that is, a website that is only accessible through the TOR network, and its actual location or server location is hidden from the public internet.

Q. Can that website be accessed from Google Chrome?

A. It cannot, unless you are using Google Chrome over a TOR network.

MR. LOCKARD: If we can turn to page, I think, 112 of Government Exhibit 1704.

Q. Can you remind us which hard drive this is of the defendant's home computer equipment?

A. So, the forensic artifact is showing the MFT being re-created on a fifth, on the C drive, and the hard drive depicted there is the Samsung SSD that was the defendant's C drive.

Q. And there are some questions about the use of a RAID 5 array. 7s this hard drive part of the RAID 5 array?

A. It is not.

Q. And what is your conclusion about what happened on this drive on May 5 of 2016?

A. It was reformatted.

Q. And from your review of the defendant's user activity and other forensic artifacts, do you have an opinion about what happened before it was formatted?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. I do.

Q. And what is that conclusion?

A. In my opinion, it was wiped before it was reformatted.

Q. The defendant asked you a number of questions about RAID 5 arrays. That's the D drive of the defendant's computer, is that right?

A. Yes.

Q. What effect would it have if a RAID 5 array were newly installed or -- let's start with newly installed. What would happen with the data on the old RAID 5 array?

A. If you removed the -- if you removed drives from the RAID 5 array and took the drives out, if you looked at any one of the individual drives, the drive -- the data would be completely recoverable because it's only a part of the data, since RAID 5 strikes data across multiple drives.

Q. And what is your ability as a forensic investigator to recover data from that type of drive?

A. From a single drive, it would be impossible.

Q. Now, we looked at some -- you were asked a number of questions about the defendant's Google search history and whether there were consistent searches in other time periods?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. I believe so, yes.

MR. LOCKARD: If we could turn to page 102 of Government Exhibit 1704.

Q. You testified earlier about a number of searches the defendant conducted for Western Digital disk-wipe utility?

A. Yes.

Q. Are you familiar with any similar type of searches in time periods prior to April and May of 2016?

A. I am not.

MR. LOCKARD: If we could go to defense exhibit 1409 and if we could go down to line -- I believe it's approximately 1846 or '47 and scan the date field.

Q. OK. So the defendant asked you some questions about the dates on his TOR browser install folder. Do you recall those questions?

A. I do.

Q. I believe you were specifically directed to dates in October of 2015?

A. I was.

Q. What is the date on line 1847?

A. April 18, 2016.

Q. And what is the name of that folder?

A. That is the folder named .TOR-browser-en\install.

Q. Mr. Berger, you were asked some questions about the defendant's use of his home server. Do you recall those questions?

A. Yes.

Q. And questions about whether that was a shared server and whether there are various forms of media that are stored and shared on that server. Do you recall those?

A. Yes.

Q. What type of internet throughput is required to share video and audio files?

A. Very high-speed connection.

MR. LOCKARD: Your Honor, if I could have just one moment, please?

Ms. Cooper, if we could please look at page 113 of Government Exhibit 1704.

Q. So, Mr. Berger, are there various events that happened between April 20, 2016, and May 5, 2016, that would impair your ability to recover forensic artifacts of the defendant's activities on his home computer?

A. Yes.

Q. Is there evidence that the defendant used the portable eraser program Eraser Portable?

A. Yes.

Q. Did the defendant use that program to securely delete a Brutal Kangaroo file?

A. Yes, he did.

Q. Were there other files that were queued for deletion but not erased through this Eraser Portable?

A. There were.

Q. Were you able to recover those files at all?

A. I was not.

Q. Did the defendant download Executioner?

A. He did.

Q. Did the defendant search for other disk-wiping utilities?

A. Yes.

Q. Including utilities for wiping solid state Samsung hard drives?

A. Yes.

Q. And on May 5, 2016, what is your conclusion about what the defendant did to his home computer?

A. He wiped and reformatted it.

Q. And we also looked at over a half-dozen other large internal hard drives that were --

MR. SCHULTE: Objection to form.

THE COURT: Sustained.

BY MR. LOCKARD:

Q. Do you recall looking at Government Exhibits 1608 through 1615?

A. Yes.

Q. What types of hard drives were those?

A. Those were internal SATA hard drives.

Q. Based on your review of those drives, was there any data stored on them?

A. There was not.

Q. Mr. Berger, who conducted the activity that led to your inability to recover forensic artifacts from that time period?

MR. SCHULTE: Objection.

THE COURT: Sustained.

MR. LOCKARD: No further questions.

THE COURT: Briefly, any recross?

RECROSS EXAMINATION

BY MR. SCHULTE:

Q. With respect to Tails, you said that there would be artifacts left on the virtual machine if it was ever booted into Tails, or if there were -- correct?

A. I testified that there would be artifacts left on the host machine if you created a virtual machine of Tails.

Q. And you found no such artifacts, correct?

A. No, because the system was reformatted.

Q. No, but you retained all the logs. All the logs were retained from that virtual machine, right?

A. If there was a Tails virtual machine, it would not have been retained if it wasn't preserved specifically.

Q. Well, about the virtual machine on the desktop, there was no artifacts that that machine was used to boot into Tails, correct?

A. You wouldn't be able to do that. You would set up a separate virtual machine to boot off the Tails ISO.

Q. Or you could boot from that virtual machine to boot to the ISO too, right?

A. You could theoretically do that, yes.

Q. There were no artifacts of that, right?

A. Not that I recall, no.

Q. With respect to the WikiLeaks URL --

MR. SCHULTE: If we can pull up slide 56, I believe, from Government Exhibit 1704. Can you do it? Thank you. Sorry.

Q. You testified that the WikiLeaks URL was needed to go to the TOR hidden service, correct?

A. Yes, WikiLeaks asked submitters to go to the dot-onion TOR hidden service.

Q. Which is represented here, right?

A. Correct.

Q. And the way you would see that here is by visiting the WikiLeaks website from the regular internet, right?

A. I'm not sure if WikiLeaks had a dot-onion that showed their main website as well.

Q. Well, I mean to see this page, you have to use the regular internet to see this, right?

A. You might be able to see this page over TOR as well.

Q. If you don't know the dot-onion address, how would you do that?

A. I mean you would need to determine what it is first, yes.

Q. How do you guess this without knowing what it is?

A. You wouldn't guess it. You would have to be told either visiting and finding it out on the regular internet or someone telling you what it is.

Q. OK. And there were no searches or visits to WikiLeaks during April and May 2016, right?

A. I don't believe so.

Q. OK. Next, the solid state drive on slide 112, you said that your testimony is that this was -- this solid state drive was wiped, correct?

A. I believe I said it was my opinion that it was wiped and reformatted, yes.

MR. SCHULTE: Can you pull up slide 112.

Q. But your forensic, through your forensic analysis, you can't determine whether this was a brand-new hard drive being used for the first time, right?

A. That's correct.

Q. OK. So it may not have been wiped or reformatted at all; it may just be completely new, correct?

A. It's possible.

Q. OK. Next, slide 102, you said in April and May that there was wiping Google searches and not before, right?

A. I believe there were no searches specific to wiping drives prior to this time period.

Q. OK. But at this time solid state drives are relatively new, correct, 2016?

A. I honestly don't recall how much market share things like that had back in 2016.

Q. OK. But once the devices became cheap enough for consumers to purchase, then searching for knowledge about those drives would be normal, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Once solid state drive technology became cheap enough, people would purchase those drives, right?

A. Yes, like any technology, the cheaper it gets, the more it's adapted.

Q. And you testified that the utilities needed to wipe those drives are different, right?

A. The recommended utilities are different, yes.

Q. OK. So it would be normal for a consumer to research that technology, right?

MR. LOCKARD: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. You notice -- you noted in defense exhibit 1407 on line 1847 the time of April 18, 2016, correct?

A. I'm not sure what you're referring to or what slide.

Q. I'm sorry. What you just talked about on your redirect.

THE COURT: I think it's 1409.

BY MR. SCHULTE:

Q. He showed you the spreadsheet of the TOR install, right?

A. Yes.

Q. OK. And you saw the April 18, 2016, date, right?

A. Yes.

Q. So if TOR was accessed and used on April 18, 2016, then that field would be updated, right?

A. I believe that date and time was specific to the install folder, so once it was installed and you were using it after the fact, it wouldn't necessarily be updated.

Q. So those folders preceding it showed the 2015 dates, though, correct?

A. I'm -- I believe there were 2015 dates that you asked me about earlier. I don't remember exactly what the paths were of those.

Q. OK. We may come back to that.

As far as the Brutal Kangaroo folder goes, you don't know if there were actually any files in that directory, correct?

A. I do not.

Q. OK. So that could have been an empty directory, right?

A. Possible.

THE COURT: All right. Mr. Schulte, I'm going to ask you just to limit yourself to new questions since you covered all that on your main cross. I do want to finish this witness before the end of the day. We're on borrowed time now.

MR. SCHULTE: Just one or two questions, and that's it.

Q. I believe the final question is with respect to the testimony about the wipe and reformat, just a clarification. Again, you can't tell whether or not the RAID was a new install or if the device was a new device, right?

A. Correct.

MR. SCHULTE: No further questions.

THE COURT: All right. Any re-redirect?

MR. LOCKARD: No, your Honor.

THE COURT: Thank you. Mr. Berger, you may step down. Please put your mask on.

(Witness excused)

THE COURT: Ladies and gentlemen, I want to thank you for giving me four extra minutes. Obviously, it makes things a lot easier just to finish with Mr. Berger, and then we can start tomorrow with a new witness. We'll call it quits there for the day. Don't discuss the case with anyone, with each other. Don't communicate about the case. Don't do any research about the case. Continue to keep an open mind.

I'm sure you can almost recite it with me at this point, but that doesn't mean that it is not absolutely important to follow all those instructions. Obviously if anyone develops Covid symptoms or you test positive, please, please, please let us know, as your colleague did the other day, but I sincerely hope, in light of everybody's negative tests this morning, that that won't happen, and we'll continue same time tomorrow.

Reminder, if you could, would, repair to the District Executive's office on the eighth floor when you come in, they'll administer a rapid test. If you would prefer to do a rapid test at home, you're welcome to do that. I just think for the next few days better to err on the side of caution and make sure we're testing on a regular basis.

With that, I wish you a very pleasant afternoon and evening.

You are excused.

(Continued on next page)

(Jury not present)

THE COURT: You may be seated.

All right. I'm just going to surmise that there might be a need to redact some of the colloquy at one of the sidebars, so I would just direct the government to review the transcript expeditiously and propose any redactions that are necessary so that we can make it public and also allow Mr. Schulte to take it with him.

Anything to discuss?

MR. DENTON: Your Honor, I think just logistically in terms of where we are and what's happening with witnesses, I think the first question we had was whether the Court had any more inclination about pressing onward and sitting on July 5 or not.

THE COURT: Well, my thought was that I would raise it with you tomorrow or Wednesday, but you're preempting that.

MR. DENTON: So, your Honor, I think just to put it in context, we assume that, as the Court ordered on Friday, we would get a sort of set of tranches of the defense witnesses to start working on moving them up here. I expect that at the rate we're going, the government will probably -- we had very much hoped to rest this week. Given that we did not even start another witness today, I think we're probably looking at resting on the first day of next week at this point.

We're also starting to run into issues with witness availability on our side, so they're -- depending on how quickly we go, we have one witness, he's not available at all next week, we may have to ask to take out of order this week just to be able to get him in. I think that if we are going to continue at a pace where the cross-examination of every witness exceeds the length of the direct, we're going to start running into more and more of those problems. And so it's just starting to exceed what we had prepared witnesses to expect.

THE COURT: All right. How does that translate with respect to July 5? The situation is, I think, obvious. Right? We have three alternates at this point. We've lost one. If we sit on July 5, I think I probably do need to excuse juror No. 8, in which case we'd be left with two alternates. I'm semiconfident that we would be OK, but we have seen in the last couple days that we may lose others as well.

MR. DENTON: I think, your Honor, we're honestly a little bit torn as between them. On the one hand, we don't want to lose an alternate. On the other hand, losing days at this point is almost as bad, and the longer this goes, the more likely we are to lose more jurors. And so I think we sort of commend the specific decision on the 5th to the Court's judgment in light of where the jury is and what the jurors are. But we just wanted to flag that, given the pace here, these concerns start to interact in not entirely helpful ways.

THE COURT: All right. Believe me, it's my desire to move things along as expeditiously as possible. I think that leaves me where I began, which is that I'm going to defer deciding that until tomorrow or the next day.

I should tell you it turns out that juror No. 13 -- I think I may have mentioned -- actually changed his plans when I asked them to but in doing so incurred some expenses, which he asked us to reimburse. I assumed that he was out of luck and would have to bear those himself, but it turns out that that might not be true; we might actually be able to reimburse him. Depending on what the scope of that authority is, maybe I can offer that to juror No. 8 as well and this problem, or at least one portion of it, goes away. Let me look into that and revisit it tomorrow or the next day, when we'll have a better sense of the pace.

I take it, am I correct, the next two witnesses are both subject to the courtroom closure protocols? Is that correct?

MR. DENTON: Yes, your Honor.

THE COURT: All right. Tomorrow morning we'll begin with those protocols in place. I assume that the CISO and the marshals will implement them. Obviously overflow will be available with the restrictions on video that I previously authorized. Anything else to raise?

From the government's perspective.

MR. DENTON: No, your Honor.

THE COURT: Mr. Schulte.

MR. SCHULTE: Yes. I had four or five things I think it's important to establish before we go into the next witness.

I think starting with this witness, the government's going to start to introduce the MCC conduct, so I wanted to raise that the government provided a late exhibit, 820-224, which is a 70-second video recorded by the government's confidential source. And he records another inmate using a cell phone, and I'm kind of in the background there. I wanted to note that this -- there's no reason, this video's very prejudicial because there's no reason for the government to show it. I don't know why the government provided it late or what the reason is for that.

THE COURT: When did you receive it?

MR. SCHULTE: I received it June 14. I don't think -- the lateness is kind of a minor issue, but I think the point is it wasn't provided before, so there was no litigation of it before until now.

MR. LOCKARD: I think there's a little record clarification, your Honor.

224 is not a new exhibit. It is a replacement of the prior version, which was lower data size and lower quality. 224 is the higher quality version of the video. But that video was introduced at the prior trial.

THE COURT: So it's the same video as what -- was it differently numbered before?

MR. LOCKARD: It's the same number. It's just the higher quality of video instead of the lower quality.

THE COURT: All right.

That sounds like a nonissue, Mr. Schulte. Do you dispute that?

MR. SCHULTE: It may be. I just, I never received 820-224 from the initial exhibits. I don't know what it was in the previous one. But I think the issue is more the contents of the video. It's prejudicial. It doesn't show me doing anything. It just shows me in prison, so I don't think there's any legitimate reason for the government to show it.

THE COURT: All right.

Mr. Lockard.

MR. LOCKARD: I have to confess I don't recall the particulars of that video, but it's certainly something that we can review, and if it's something we can avoid an issue about, maybe we'll decline to introduce it. But let's take a look at it first.

THE COURT: All right. You know better than I where and how you were planning to use it. If there's a reason for it, I'm open to hearing it, but if all it does is show that Mr. Schulte's in prison, I don't think there's much point to it. Why doesn't the government alert Mr. Schulte and me before it uses it, and then we can hash it out further.

Next.

MR. SCHULTE: The next thing I wanted to raise is the next witness, Weber, was one of the witnesses that I notified the Court about going beyond the cross, so I'm not sure how long the government intends to have him testify on direct, but if I'm able to get in all of the evidence that I'd like to through this witness, it would substantially cut down any witnesses that I would call. So it would make the defense case much shorter. So I don't know -- and after this witness, I expect the others to be much shorter as to cross and stuff like that. So I don't know -- I just want to notify the Court. I don't know if the Court would rather me re-call the witness, or --

THE COURT: No. In general, I would rather you go beyond the scope and deal with whatever testimony you wish to elicit when he's on the stand, particularly as to the next witness, who is subject to the courtroom-closure protocols. So I appreciate your giving me a heads-up on that and certainly hope that after this witness the crosses do become shorter.

Go ahead.

MR. SCHULTE: OK. The next issue is the MCC notebooks that the government provided. I think there's Federal Rule of Evidence 106, which requires introduction of the remaining pages. So the government selected a couple pages from several of the exhibits, and I would like to introduce more of the notebooks to be able to show it in context and also colored versions of the cover. So I don't know if the Court's inclination is to have me have defense exhibits named the same thing or if the government and defense should just have a combined exhibit of those.

THE COURT: Mr. Lockard.

MR. LOCKARD: Well, those notebooks are the defendant's statements, so I don't think they're admissible by him as a defense exhibit in any event. They're also heavily redacted principally due to the assertion of attorney-client privilege, which was not litigated; it was just accepted. So it's not likely that he can even introduce the entire notebook unless he's going to waive privilege at this point. And he has not identified what particular portions of these documents are required for completeness, so I think our position is we object.

THE COURT: All right.

Mr. Schulte, I think I'm inclined to agree with Mr. Lockard, at least the last point, which is that I don't think Rule 106 provides an avenue to introduce the notebooks in their entirety unless you can demonstrate that that is necessary to understand the portions that the government is admitting and that it's required out of fairness, etc., which I find hard to believe that you would be able to sustain as to the notebooks as a whole. Whether there are particular portions of it to put the excerpts that are coming into evidence in context is a different question, but I think the onus is on you to identify those and show them to the government and, if there's any dispute, to present it to me to decide whether it is actually admissible under Rule 106.

MR. SCHULTE: Yeah, so I provided the government copies of the entire notebooks, and then recently, I cut down and selected the specific portions that I think are relevant. Specifically, for example, "Malware of the Mind" document, a lot of it is talking about the criminal justice system, and they picked out, like, one or two points which don't establish anything at all the about what the point of the document is.

THE COURT: Can I ask a question. When are these documents, the excerpts coming into evidence? I assume it's not through the next witness. Or it is?

MR. LOCKARD: The next witness is going to talk about some particular aspects of what's in the notebooks.

THE COURT: OK.

Mr. Schulte, you're saying that you did identify for the government excerpts that you believe are admissible under Rule 106?

MR. SCHULTE: I initially provided them the entire exhibits, but today, I provided them -- I cut down the specific portions that I thought were relevant to show.

THE COURT: OK.

Mr. Lockard, have you seen those?

MR. LOCKARD: I think we've seen the disk. I don't think we've seen the documents.

THE COURT: All right. I think we need to take it one step at a time. Obviously, the government should review those. If there's no objection, then it's one thing. If there is an objection, then we'll have to hash it out, but I do think that this is something that should've been done pretrial, likely through motions *in limine*. Given that the admissibility of these documents, in whole, in part, the privileged nature of them or lack thereof, so on and so forth, have been litigated over and over and over, it should not have come as a surprise that the government was introducing portions of it, and if you thought other portions should have been admitted out of fairness, I really think it was incumbent upon you to identify those earlier in the process. Be that as it may, the government will review it and we'll discuss it tomorrow.

Next.

MR. SCHULTE: And then one other thing about the redactions is I wanted to note for the Court, specifically, Government Exhibit 806 page 2, that the government redacted a portion of the notebook that shows that this was intended for Judge Crotty, but this wasn't redacted pursuant to privilege and it wasn't redacted pursuant to classification. It was redacted after the fact, so I think that that redaction should be taken out of the document. I don't know if the government's been able to review that yet, but I noticed it to the government.

The production provided to me in unclassified discovery shows the specific statement, which is something -- something to your Honor, some statement about that. So that was never redacted for privilege. It wasn't classified. And then, and the government didn't redact it for its exhibits.

THE COURT: This is in Government Exhibit 806, you said?

MR. SCHULTE: 806, page 2, yes.

THE COURT: Page 2 in the PDF? It seems to be page 40 of 95 in the PDF.

MR. SCHULTE: Yes. Page 2 in the exhibit but page whatever it is in the overall.

THE COURT: OK. I am not seeing it as redacted here. I don't know what Mr. Schulte's talking about, but Mr. Lockard, can you enlighten me?

MR. DENTON: Your Honor, there were a number of redactions that were taken at the request of the defendant's prior counsel, including references like that and references to child pornography and other references that were not for privilege or classification. So I can't say I remember that one in particular, but we got a long list of previously active counsel of things to redact there, so I imagine that's what that is.

THE COURT: To the extent Mr. Schulte is asking you to revisit this particular one, do you have a position on it, or do you want to review it?

MR. DENTON: I'd certainly like to review it, your Honor.

THE COURT: All right. Why don't you take a look at that, and if you have no objection to unredacting whatever he's referring to, then I suppose let's prepare a new version.

Mr. Schulte, do you want to make clear precisely what you're talking about, or did you present that to the government?

MR. SCHULTE: I can quote the sentence if that's helpful.

THE COURT: Where does it appear on the page? There are three redaction blocks here?

MR. SCHULTE: I believe it's at the top, says something to the effect of there's been no reason over the past year that we should not have access, something like -- that's how it starts.

THE COURT: All right. The government should review that. And again if there's no dispute, great. If there is, I will resolve it.

Anything else, Mr. Schulte?

MR. DENTON: I'm sorry, your Honor. I can say having looked at it we will object to that. It's the defendant's own statement that prosecutors have lied and that evidence was withheld from him. Even putting aside the privilege issue about whether it was addressed to the Court, we think it's obviously inadmissible.

MR. SCHULTE: The relevance is that the statement that's made right after that line is being included into the letter to the judge. So to the fact that the government wants to show that, they should show the entire letter or they should redact that whole page.

THE COURT: All right. Maybe my law clerk can enlighten me, but does anyone know where I can find the unredacted version of this page so that I can review the entirety of it in context?

MR. LOCKARD: We can provide it if you don't already have a copy of it.

THE COURT: All right. I think we have a paper copy. I suppose if you have it in electronic form and it can be transmitted electronically, then it might facilitate things. But if not, we'll recover the paper copy.

MR. LOCKARD: Yes, your Honor. Ms. Cooper can make that happen.

THE COURT: Great.

Thank you, Ms. Cooper.

Anything else, Mr. Schulte?

MR. SCHULTE: Yes. A couple of other things.

With this next witness, I may need to reference classified exhibit 1, so I'm not sure how the Court wants to handle that. I wanted to bring it to your attention.

THE COURT: Well, I think the devil is in the details of what reference means.

MR. SCHULTE: Yes.

THE COURT: To the extent that the request is to display any portions of it, I think we've litigated that question.

MR. SCHULTE: I'm sorry?

THE COURT: I said to the extent that the request is to display portions of it, I think that we have litigated that question and it's not necessary. But what do you intend to do with it?

MR. SCHULTE: Yes. The pages about the Bartender that were never declassified, I would like to go through those issues. So I -- I think that the Court denied the application pursuant to CIPA to declassify the information. So it's still classified, so I wanted to be able to reference that with the witness.

MR. DENTON: Obviously, your Honor, he can't elicit classified information that was not noticed and approved by the Court. The fact that some portion of it is in evidence as a classified exhibit does not give him license to just simply declare it in court.

MR. SCHULTE: My understanding was that it was admitted as classified exhibit and we would use the silent witness rule to go through that information in some manner. That was my understanding. Is that not the case?

THE COURT: I think if you intended to elicit it and elicit testimony about it, that was definitely something that you had to notice prior to trial, because it does raise obviously significant issues, and the silent witness rule with respect to actual testimony is very different than admitting the exhibit, which I've approved, for reasons that I've laid out in an opinion already. But excluding the public from a courtroom altogether for testimony of a witness is a very, very different matter and raises entirely different things, and to the extent that you wanted to do that, it was incumbent upon you to notice it before trial and for us to litigate the permissibility and extent of which you were allowed to do that, and you didn't. And I certainly didn't approve doing it. So I think that ship has sailed, and you may not.

MR. SCHULTE: No. We did litigate it, but you denied it.

THE COURT: OK. That sort of makes it a worse situation for you rather than a better, so I think that --

MR. SCHULTE: You denied the declassification of it, but my understanding was I could still, because it's in evidence and I could still reference that. Is that not the case?

THE COURT: That is not the case. I think that was quite clear from all of the litigation over the admission of Government Exhibit 1 -- that being admitted as a classified exhibit meant it was not being discussed in the courtroom, and if you had any intention of eliciting testimony about any portions of it, we did litigate that. I would have to go back to my ruling to see exactly what you're referring to and whether you noticed it or not, but I certainly didn't approve any request, so either you didn't notice it or I denied it. And in either case you're not doing it.

So what's next?

MR. SCHULTE: OK. The next thing I wanted to raise is I think we discussed it a little bit with the IRC chats that are admitted, were not admitted with year and so it's very misleading to the jury. And also, as I said before, that there's massive, like, 1,200 pages and a thousand pages on several exhibits and I sent a letter to the government about it, but I don't think that's been resolved so to the degree that these are going to be coming in, I just think we should resolve that now, unless the government intends to not object.

THE COURT: Can somebody tell me what exhibit we're talking about?

MR. LOCKARD: These are the 1405-1, etc., series of exhibits. Mr. Schulte did raise this by letter in sort of work flow management of issues. We had not yet resolved it, because it was not coming up over the last couple weeks of trial, but we expect to be able to resolve it. No. 1, I think we will probably withdraw a couple of those exhibits, and No. 2, with respect to dates, we think we will resolve that issue through future witness testimony.

THE COURT: All right. Great. Doesn't sound like there's anything for me to weigh in on just yet, but obviously, please let Mr. Schulte know as soon as you know which of these you're withdrawing. And otherwise, with respect to the year issue, I'll wait and see what sort of foundation is laid. With respect to any particular ones being either irrelevant or prejudicial, we'll take that up after the government reports to Mr. Schulte which it's withdrawing.

So, Mr. Schulte, the burden's on the government first to clarify what they intend to do and then, Mr. Schulte, on you to raise any objections with respect to whatever remains.

What's next?

MR. SCHULTE: Yes. Does the Court want to go through the issue with the last exhibit I had and Mr. Berger, any of that now, or you want to defer to that some other time?

(Continued on next page)

THE COURT: I'm happy to do it now. I mean, obviously if you have any application to recall Mr. Berger you can make that application but I think there were two issues, one of which was scope but, as you pointed out, to the extent that he was one of the witnesses you had previously identified that he wished to go beyond the scope of that is a fair point and I appreciate your reminding me of that.

The other issue is that I don't think he was a competent witness to testify about that exhibit. He indicated that he was not familiar with that particular exhibit, he was not familiar with that, with how Verizon reported or maintained its NetFlow log. He was very clear that different providers do it differently so I think attempting to use him to explain an exhibit that he was very clear that he was not familiar with was not proper and I don't see how you can recall him to do that given that, again, he said he wasn't familiar with it.

MR. SCHULTE: Yes. So I think he was playing games a little bit about it because the NetFlow logs were very clear but I can call a Verizon witness to --

THE COURT: I mean, the exhibit is in evidence. To the extent that it doesn't require an expert to opine or explain it then you can argue from it. To the extent that it does require someone to interpret the records, Mr. Berger wasn't the proper witness to do it because he said he wasn't familiar with it. Now, you may argue that that was incredible testimony. You can argue that to the jury, if you wish, that's the jury's prerogative to decide but given that that was his testimony, it was improper to try and use him to try and elucidate what was in the logs.

MR. SCHULTE: I think Mr. Berger is in the room right now so we may just have to address it later.

THE COURT: Why don't I ask Mr. Berger to step out and then we can continue to address it.

MR. SCHULTE: OK.

THE COURT: He has stepped out.

MR. SCHULTE: OK, so I think what I would intend to do is introduce evidence about what a NetFlow log is, the information he should already know, especially if he is working on the investigation. As Mr. Leedom testified, it is the primary document that you would review so the fact that he doesn't know what this is is just not realistic, so showing him technical definition of NetFlow or even recalling Mr. Leedom because Mr. Leedom seemed to talk about it and understand the technical details of it, but the point was to call one of the government witnesses to go through this document.

THE COURT: OK, but he testified that he did know what NetFlow was, he answered that question, and he explained that different providers record it differently, and without knowing more he wouldn't be able to interpret that document. So it seems to me that you have gotten out of Mr. Berger what you could get out of him on that subject. And, again, maybe there is a witness that you can call as part of your case to elicit more for or make more of those records, but I don't think that recalling Mr. Berger is the proper course.

You had ample opportunity to ask those questions of Mr. Leedom. The fact that you didn't, that ship has sailed.

MR. SCHULTE: So I think the problem may be then we discussed a little bit about my testimony and how I would testify as an expert, or if the document requires expert testimony so that may be an issue. When I am testifying I could testify to what the document is and what it would show, but if that --

THE COURT: That sure sounds like expert testimony to me and I don't think you noticed any expert testimony of your own before trial.

MR. SCHULTE: I don't think as a defendant that I am required to show expert testimony until I am about to make the decision to testify, it was my understanding, unless there is some other case precedent or something.

THE COURT: Mr. Denton, you are standing which suggests that you have something to say.

MR. DENTON: I just wanted to note, your Honor, that I think there is a little bit of gamesmanship happening here. We informed the defendant when we agreed to stipulate to the authenticity of the records that we did believe that these were records that required expert testimony to interpret them and that no notice of any kind had been given to that effect so I think that's largely why we are playing this game here. Also, there is no exception to the expert notice rule for the defendant. He can make the decision whether or not to testify but if he intends to offer expert conclusions he is subject to the same notice rules as anybody else.

THE COURT: All right. I confess I have never researched that particular legal question but it would surprise me if that were not the law. Mr. Schulte, if you think it is otherwise I am certainly glad for you to point me to authority, but otherwise I would think you are subject to the same requirements as any expert. Obviously noticing an expert doesn't mean that you are committing to call the expert, it just means that you are putting the government on notice of your intent and if there are any issues to litigate about the expertise or scope of testimony, then it permits the government to do it but it doesn't bind you to testify, it just requires that you provide notice.

MR. SCHULTE: So I think the issue is basically surrounding this document is the defense never believed that there is any expert testimony required. If you saw in the field there is a bytes field, it shows the amount of data that's been transferred or received. If you add all of that up it is significantly smaller than 200 gigabytes so the government's case is not possible. All it takes is adding up -- I noticed this to the Court in an *ex parte* letter but if you just add up those fields in Excel through a sum add, then that gives you the number. It was never something that we believed required expert testimony to add numbers together.

THE COURT: I think it does require expert testimony to explain that that's what that column means and I don't think that that's within a layperson's understanding. And you tried to do that with Mr. Berger but his answer was that he is not familiar with these particular documents or how Verizon does it.

I also would point out -- the government can correct me if I am wrong -- I don't think the government has -- granted, the government doesn't have any smoking gun evidence of how the data was transmitted if you transmitted it to WikiLeaks but I don't think the government has actually taken a definitive view on how you transmitted it. I think their view is that, for instance, you explored, I would imagine, the use of Tails and TOR but it may well be that, as Mr. Berger testified, that you didn't finish the job that way because it was a large file and it wouldn't have been feasible to do it for precisely the way you are describing, and that you availed yourself of some other transmission that wouldn't be inconsistent with that. So in that sense, I'm not sure it, quote unquote, proves the impossibility of the government's theory.

MR. SCHULTE: I think it goes to the indictment and specifically the time frame that the government has alleged. You can't just say, well, at some random time this data was transmitted. So specifically showing that this time and data wasn't transmitted it there or even expanding it to other times it just goes to the defense's case. How the government chooses to respond to that is up to the government, but I still think it is a very strong point to the defense and -- to the degree of interpreting the documents I think the problem is Verizon never provided any data and the way that that flow log worked, this is how it should be -- there is only one way it should be interpreted. So I'm not sure -- I don't know what can be done with that, but. I mean, if Verizon is not providing any notice or any information about how to interpret it then the point is you should use standard measurements for how NetFlow works, in general.

THE COURT: Mr. Schulte, I think this is a problem of your own making. You didn't notice your own expert and it doesn't sound like right now you have an intention to call a Verizon expert. What you did, you tried to use the government's expert to basically do that work for you and it turns out that Mr. Berger, whether credibly or not -- I don't know, it is up to you and the jury -- you to argue and for the jury to decide -- said he is not familiar with these and wasn't in a position to opine about them.

So I'm not saying you can't make use of this. I'm not saying you can't make this argument. But, it is incumbent upon you to do what you need to do to make it so if that means calling an expert, whether it is too late for not is a different question. Whether it means calling a witness from Verizon who may simply be able to say what the data means then you can make the argument, or whether it means that you can simply argue from a document separate questions. But, to the extent that the question is whether you can recall Mr. Berger to try and elicit it from him, I think you have extracted from him what there was to extract and there is nothing further to do.

MR. SCHULTE: OK.

I think a Verizon witness who interprets records is not considered an expert though, right?

THE COURT: I think if you call a Verizon witness who says these are Verizon records and who says this is what each of these fields means, that would not be expert testimony. To the extent that that allows you to make an argument to the jury that adding that up would reveal the maximum amount of data that was transmitted over your network in that period of time, it doesn't -- isn't big enough to correspond to this, I suppose you can make that argument. It does sound to me like there are steps in that argument that would probably require some sort of expertise but I don't know, we are not there yet. Certainly -- government, you can tell me if you disagree -- I think having a Verizon witness testify just as a matter of factually what each of those columns means would not be expert testimony. How that translates is a different story and may or may not require another level of expertise.

Any disagreement with that?

MR. DENTON: No, your Honor, although again I would note the defendant has been the one who has been asking for stipulations and all of that. We thought we were making life easier this way. If he now wants to start calling records custodians we are going to be in a whole different ball game.

THE COURT: Understood. Maybe there is a stipulation to be had here since Mr. Schulte wasn't able to get from Mr. Berger what he wanted. If his plan would be to call a Verizon witness and there is no dispute about what that witness would say, then maybe the parties would stipulate to that. But I think that is sort of where we are on this issue.

Anything further on that, Mr. Schulte?

MR. SCHULTE: No. I think that's it.

THE COURT: Anything further at all?

MR. LOCKARD: Not from the government, your Honor.

MR. SCHULTE: No. Nothing further.

THE COURT: All right. So a few issues to revisit tomorrow. Again, just reminder for the government to review the transcript today as quickly as possible, and if you have stakeholders you need to do that, make sure they do it.

I will see you tomorrow at the same time, same place. Thank you.

(Adjourned to June 28, 2022 at 9:00 a.m.)

INDEX OF EXAMINATION

DEFENDANT EXHIBITS